

October 14-18, 2024
Salt Lake City, UT, USA



Association for
Computing Machinery

Advancing Computing as a Science & Profession



CCS '24

Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security

Sponsored by:

ACM SIGSAC

General Chairs:

Bo Luo (University of Kansas, USA)

Xiaoqing Liao (Indiana University Bloomington, USA)

Jun Xu (University of Utah, USA)

Program Chairs:

Engin Kirda (Northeastern University, USA)

David Lie (University of Toronto, Canada)

Proceedings Chairs:

Fengwei Zhang (SUSTech, China)

Dongpeng Xu (University of New Hampshire, USA)



**Association for
Computing Machinery**

Advancing Computing as a Science & Profession

The Association for Computing Machinery

**1601 Broadway, 10th Floor
New York, NY 10019-7434**

Copyright © 2024 by the Association for Computing Machinery, Inc. (ACM).

Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page.

Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from: permissions@acm.org or Fax +1 (212) 869-0481.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through www.copyright.com.

ISBN: 979-8-4007-0636-3

Additional copies may be ordered prepaid from:

ACM Order Department

PO Box 30777
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)

+1-212-626-0500 (Global)

Fax: +1-212-944-1318

E-mail: acmhelp@acm.org

Hours of Operation: 8:30 am – 4:30 pm ET

Cover photo obtained from bigstockphoto.com

Message from the ACM CCS 2024 General Co-Chairs

It is with great enthusiasm that we, on behalf of the Organizing Committee, invite you to join us for the 31st ACM SIGSAC Conference on Computer and Communications Security (CCS), a premier security and privacy conference where researchers, practitioners, and educators come together to present, learn, and debate research, innovation, and trends in the field of Computer and Communications Security and Privacy.

This year, we are proud to introduce our conference theme to be “Inclusion, Mentorship, Community.” These three pillars reflect our collective commitment to fostering a vibrant, supportive, and forward-thinking environment within the CCS community. Particularly, we host our inaugural *Doctoral Symposium*, which offers PhD students a unique platform to receive timely, constructive feedback on their dissertation research from leading experts in our community. Additionally, our first-ever *Diversity, Equity, and Inclusion (DEI) Workshop* is designed to cultivate a culture that embraces diversity and champions equity in our field. Moreover, understanding the importance of guidance and support, we have organized panels focusing on *Student Mentoring*, *Faculty Mentoring*, and *Public Service*. These panels are designed to facilitate mentorship connections, share valuable experiences, and encourage service that extends the impact of our work beyond academia. These new initiatives are also opportunities to strengthen the bonds within our CCS community.

Regarding the main conference, this year’s main conference is our *largest* ever, featuring 328 paper presentations that showcase the latest research and developments in our field. We are also honored to have two distinguished keynote speakers: Dr. Dan Boneh and Dr. Gene Tsudik, who will share their invaluable insights and perspectives on pressing topics in security and privacy. Additionally, 18 specialized workshops will take place on the pre-conference and post-conference days, providing platforms for focused discussions and collaborations on numerous specialized topics.

We would like to extend our deepest gratitude to all the authors, program chairs, track chairs, co-located event organizers, program committee members, artifact evaluation committee members, post/demo committee members, and external reviewers, who have dedicated their time and effort to make this conference possible. Your commitment and hard work are the backbone of CCS 2024, and it is through your contributions that we continue to thrive as a community. Also, we would like to thank ACM, SIGSAC, organizing committee members and our sponsors for their support of CCS 2024. This conference would not have been possible without their dedication and commitment.

Welcome to Salt Lake City! We hope that you will find CCS 2024 interesting and thought-provoking, providing you with a valuable opportunity to share ideas with other researchers and practitioners around the world.

Bo Luo

*CCS’24 General Co-Chair
University of Kansas*

Xiaoqing Liao

*CCS’24 General Co-Chair
Indiana University*

Jun Xu

*CCS’24 General Co-Chair
University of Utah*

Welcome from the ACM CCS 2024 Program Co-Chairs

Welcome to the proceedings of the 31st ACM Conference on Computer and Communications Security (CCS). The task of the Program Committee, led by the Program Chairs and the Track Chairs, was to select the papers that would appear in this edition of the conference. Keeping with the tradition, we had two reviewing cycles, with submission deadlines in January and April, each with a roughly 2.5-month review cycle. This year, due to a tighter schedule as the conference was taking place mid October instead of November as in 2023, the submission Cycles A and B had to overlap. Also, as in previous years, due to the record number of papers submitted, and to give to the authors the opportunity to submit their papers elsewhere, some papers were rejected early in the process, as the result of receiving two negative reviews. For the remaining papers, the authors were given the opportunity to submit a rebuttal to address specific concerns of the reviewers. By the end of each cycle, each submitted paper was marked for acceptance, conditional acceptance (shepherding), rejection, or revision. Papers in the last category were allowed to be resubmitted for another round of review, under the assumption that they would be accepted if the requirements set by the reviewers were met satisfactorily. All submissions were reviewed by a Program Committee of over 527 security and privacy experts from around the world, along with many expert sub-reviewers from outside the committee. The Program Co-Chairs were assisted by thirteen Track Chairs: Yuan Tian, Jason Polakis, Aanjhan Ranganathan, Catalin Hritcu, Yinqian Zhang, Melek Onen, Katerina Mitrokotsa, Reza Shokri, Murat Kantarcioglu, Blase Ur, Gianluca Stringhini, Stefanie Roos, and Wouter Lueks, who are recognized experts in their respective subfields. The Track Chairs were also involved in selecting the top reviewers and the distinguished paper awards.

The January cycle received 748 submissions, with 75 papers accepted (possibly with shepherding). An additional 59 papers were chosen for revision, with 57 of those eventually being accepted after the revised version was submitted. Of the papers that were rejected, 362 were rejected early. A total of 1216 papers were submitted to the April cycle, with 122 papers accepted (possibly with shepherding) and 77 papers chosen to be revised. From the latter group, 74 papers were eventually accepted. Of the rejected papers, 631 were rejected early. Altogether, 328 out of 1964 submissions were accepted, for an acceptance rate of 16.7%. The accepted papers cover a wide range of topics in security, including web security, machine learning, network security, formal methods, software security, IoT/CPS security, applied cryptography, privacy and anonymity, security usability and measurement, blockchain, and distributed systems security.

We thank the Track Chairs, PC members, and external reviewers for their contributions to the conference and for their dedication to high-quality reviewing. We are also extremely grateful to the General Chairs, Bo Luo, Xiaojing Liao, and Jun Xu, for organizing the conference, the Proceedings Chairs, Fengwei Zhang and Dongpeng Xu, the Workshop Chairs, Christophe Hauser and Aurore Fass, Poster/Demo chairs, Sara Foresti and Xiaoyan Sun, as well as the many other chairs that helped us the diversity of tasks that are critical for establishing a program of this size. We could not have done all of this without you!

We also thank all the authors for submitting their outstanding research to ACM CCS. We hope you enjoy the conference!

Engin Kirda
CCS'24 Program Co-Chair
Northeastern University

David Lie
CCS'24 Program Co-Chair
University of Toronto

Table of Contents

2024 ACM CCS Organization	xli
CCS 2024 Program Committee	xliii
CCS 2024 External Reviewers	1
CCS 2024 Artifact Evaluation Committee	lv
CCS 2024 Sponsor, Patrons, & Supporters	lvii

Keynote Talks

- **Cryptography and Computer Security: A View From the Year 2100**..... 1
Dan Boneh (*Stanford University*)
- **Staving off the IoT Armageddon** 2
Gene Tsudik (*University of California, Irvine*)

Session 1-1: Verification, Secure Architectures, and Network Security

- **Verifiable Security Policies for Distributed Systems**..... 4
Felix A. Wolf (*Department of Computer Science, ETH Zurich*),
Peter Müller (*Department of Computer Science, ETH Zurich*)
- **Libra: Architectural Support For Principled, Secure And Efficient Balanced Execution On High-End Processors** 19
Hans Winderix (*DistriNet, KU Leuven*), Marton Bognar (*DistriNet, KU Leuven*),
Lesly-Ann Daniel (*DistriNet, KU Leuven*), Frank Piessens (*DistriNet, KU Leuven*)
- **Compositional Verification of Composite Byzantine Protocols**..... 34
Qiyuan Zhao (*National University of Singapore*), George Pirlea (*National University of Singapore*),
Karolina Grzeszkiewicz (*Yale-NUS College*), Seth Gilbert (*National University of Singapore*),
Ilya Sergey (*National University of Singapore*)
- **Byzantine-Secure Relying Party for Resilient RPKI**..... 49
Jens Frieß (*TU Darmstadt & ATHENE*), Donika Mirdita (*TU Darmstadt & ATHENE*),
Haya Schulmann (*Goethe-Univ. Frankfurt & ATHENE*), Michael Waidner (*TU Darmstadt & ATHENE*)

Session 1-2: HW & CPS: Microarchitectural Attacks and Side Channels

- **SysBumps: Exploiting Speculative Execution in System Calls for Breaking KASLR in macOS for Apple Silicon**..... 64
Hyerean Jang (*Korea University*), Taehun Kim (*Korea University*),
Youngjoo Shin (*Korea University*)
- **TDXdown: Single-Stepping and Instruction Counting Attacks against Intel TDX** 79
Luca Wilke (*University of Lübeck*), Florian Sieck (*University of Lübeck*),
Thomas Eisenbarth (*University of Lübeck*)
- **Cross-Core Interrupt Detection: Exploiting User and Virtualized IPLs** 94
Fabian Rauscher (*Graz University of Technology*), Daniel Gruss (*Graz University of Technology*)
- **Spec-o-Scope: Cache Probing at Cache Speed** 109
Gal Horowitz (*Tel Aviv University*), Eyal Ronen (*Tel Aviv University*),
Yuval Yarom (*Ruhr University Bochum*)

Session 1-3: ML and Security: Machine Learning for Security

- **Training Robust ML-based Raw-Binary Malware Detectors in Hours, not Months** 124
Keane Lucas (*Carnegie Mellon University*), Weiran Lin (*Carnegie Mellon University*),
Lujo Bauer (*Carnegie Mellon University*), Michael K. Reiter (*Duke University*),
Mahmood Sharif (*Tel Aviv University*)

- **TREC: APT Tactic / Technique Recognition via Few-Shot Provenance Subgraph Learning** 139
Mingqi Lv (College of Computer Science and Technology, Zhejiang University of Technology),
Hongzhe Gao (College of Computer Science and Technology, Zhejiang University of Technology),
Xuebo Qiu (College of Computer Science and Technology, Zhejiang University of Technology),
Tieming Chen (College of Computer Science and Technology, Zhejiang University of Technology),
Tiantian Zhu (College of Computer Science and Technology, Zhejiang University of Technology),
Jinyin Chen (College of Information Engineering, Zhejiang University of Technology),
Shouling Ji (College of Computer Science and Technology, Zhejiang University)
- **SAFARI: Speech-Associated Facial Authentication for AR/VR Settings via Robust Vibration Signatures**..... 153
Tianfang Zhang (Rutgers University), Qiufan Ji (New Jersey Institute of Technology),
Zhengkun Ye (Temple University), Md Mojibur Rahman Redoy Akanda (Texas A&M University),
Ahmed Tanvir Mahdad (Texas A&M University), Cong Shi (New Jersey Institute of Technology),
Yan Wang (Temple University), Nitesh Saxena (Texas A&M University), Yingying Chen (Rutgers University)
- **KnowGraph: Knowledge-Enabled Anomaly Detection via Logical Reasoning on Graph Data** 168
Andy Zhou (UIUC), Xiaojun Xu (Bytedance Research), Ramesh Raghunathan (eBay),
Alok Lal (eBay), Xinze Guan (eBay), Bin Yu (UC Berkeley), Bo Li (UIUC)

Session 1-4: HW & CPS: (Micro)Architecture Security

- **Principled Microarchitectural Isolation on Cloud CPUs** 183
Stavros Volos (Azure Research, Microsoft), Cédric Fournet (Azure Research, Microsoft),
Jana Hofmann (Azure Research, Microsoft), Boris Köpf (Azure Research, Microsoft),
Oleksii Oleksenko (Azure Research, Microsoft)
- **Interstellar: Fully Partitioned and Efficient Security Monitoring Hardware Near a Processor Core for Protecting Systems against Attacks on Privileged Software** 198
YongHo Song (Korea Advanced Institute of Science and Technology & CySecuLab),
Byeongsu Woo (Korea Advanced Institute of Science and Technology & CySecuLab),
Youngkwang Han (Korea Advanced Institute of Science and Technology & CySecuLab),
Brent ByungHoon Kang (Korea Advanced Institute of Science and Technology & CySecuLab)
- **μ CFI: Formal Verification of Microarchitectural Control-flow Integrity** 213
Katharina Ceesay-Seitz (ETH Zurich), Flavien Solt (ETH Zurich), Kaveh Razavi (ETH Zurich)
- **Crystalor: Recoverable Memory Encryption Mechanism with Optimized Metadata Structure**..... 228
Rei Ueno (Tohoku University), Hiromichi Haneda (Tohoku University), Naofumi Homma (Tohoku University),
Akiko Inoue (NEC Corporation), Kazuhiko Minematsu (NEC Corporation)

Session 1-5: Privacy and Anonymity: Privacy in Federated ML

- **Camel: Communication-Efficient and Maliciously Secure Federated Learning in the Shuffle Model of Differential Privacy** 243
Shuangqing Xu (Harbin Institute of Technology, Shenzhen),
Yifeng Zheng (Harbin Institute of Technology, Shenzhen),
Zhongyun Hua (Harbin Institute of Technology, Shenzhen)
- **S²NeRF: Privacy-preserving Training Framework for NeRF**..... 258
Bokang Zhang (The Chinese University of Hong Kong, Shenzhen),
Yanglin Zhang (The Chinese University of Hong Kong, Shenzhen), Zhikun Zhang (Zhejiang University),
Jinglan Yang (The Chinese University of Hong Kong, Shenzhen),
Lingying Huang (Nanyang Technological University),
Junfeng Wu (The Chinese University of Hong Kong, Shenzhen)
- **\$DPM\$: Clustering Sensitive Data through Separation** 273
Johannes Liebenow (Universität zu Lübeck), Yara Schütt (Universität zu Lübeck),
Tanya Braun (University of Münster), Marcel Gehrke (University of Hamburg),
Florian Thaeter (Independent), Esfandiar Mohammadi (Universität zu Lübeck)
- **S-BDT: Distributed Differentially Private Boosted Decision Trees** 288
Thorsten Peinemann (Universität zu Lübeck), Moritz Kirschke (Universität zu Lübeck), J
oshua Stock (University of Hamburg), Carlos Cotrini (ETH Zurich),
Esfandiar Mohammadi (Universität zu Lübeck)

Session 1-6: Privacy and Anonymity: Differential Privacy I

- **Cross-silo Federated Learning with Record-level Personalized Differential Privacy** 303
Junxu Liu (*Renmin University of China*), Jian Lou (*Zhejiang University*), Li Xiong (*Emory University*),
Jinfei Liu (*Zhejiang University*), Xiaofeng Meng (*Renmin University of China*)
- **Benchmarking Secure Sampling Protocols for Differential Privacy** 318
Yucheng Fu (*University of Virginia*), Tianhao Wang (*University of Virginia*)
- **Smooth Sensitivity for Geo-Privacy** 333
Yuting Liang (*Hong Kong University of Science and Technology*),
Ke Yi (*Hong Kong University of Science and Technology*)
- **Metric Differential Privacy at the User-Level via the Earth-Mover's Distance** 348
Jacob Imola (*University of Copenhagen*), Amrita Roy Chowdhury (*University of Michigan, Ann Arbor*),
Kamalika Chaudhuri (*University of California, San Diego*)

Session 1-7: Blockchains, Authentication, and Distributed Systems

- **Nakamoto Consensus under Bounded Processing Capacity** 363
Lucianna Kiffer (*ETH Zürich*), Joachim Neu (*Stanford University*), Srivatsan Sridhar (*Stanford University*),
Aviv Zohar (*The Hebrew University*), David Tse (*Stanford University*)
- **Data Independent Order Policy Enforcement: Limitations and Solutions** 378
Sarisht Wadhwa (*Duke University*), Luca Zanolini (*Ethereum Foundation*),
Aditya Asgaonkar (*Ethereum Foundation*), Francesco D'Amato (*Ethereum Foundation*),
Chengrui Fang (*Zhejiang University*), Fan Zhang (*Yale University*), Kartik Nayak (*Duke University*)
- **Securing Lightning Channels against Rational Miners** 393
Lukas Aumayr (*TU Wien, Christian Doppler Laboratory Blockchain Technologies for the Internet of Things*),
Zeta Avarikioti (*TU Wien, Common Prefix*),
Matteo Maffei (*TU Wien, Christian Doppler Laboratory Blockchain Technologies for the Internet of Things*),
Subhra Mazumdar (*Indian Institute of Technology Indore*)
- **Interactive Multi-Credential Authentication** 408
Deepak Maram (*Mysten Labs, Cornell Tech*), Mahimna Kelkar (*Cornell Tech*), Ittay Eyal (*Technion*)

Session 2-1: Network Security: The Internet Infrastructure

- **Towards Fine-Grained Webpage Fingerprinting at Scale** 423
Xiyuan Zhao (*INSC & BNRist, Tsinghua University*), Xinhao Deng (*INSC & BNRist, Tsinghua University*),
Qi Li (*INSC, Tsinghua University & Zhongguancun Laboratory*), Yunpeng Liu (*INSC, Tsinghua University*),
Zhuotao Liu (*INSC, Tsinghua University & Zhongguancun Laboratory*), Kun Sun (*IST, George Mason University*),
Ke Xu (*DCST, Tsinghua University & Zhongguancun Laboratory*)
- **Understanding Routing-Induced Censorship Changes Globally** 437
Abhishek Bhaskar (*Georgia Institute of Technology*), Paul Pearce (*Georgia Institute of Technology*)
- **Internet's Invisible Enemy: Detecting and Measuring Web Cache Poisoning in the Wild** 452
Yuejia Liang (*Tsinghua University*), Jianjun Chen (*Tsinghua University & Zhongguancun Laboratory*),
Run Guo (*Tsinghua University*), Kaiwen Shen (*Tsinghua University & Clouditera Inc*),
Hui Jiang (*Tsinghua University & Baidu Inc*), Man Hou (*Zhongguancun Laboratory*),
Yue Yu (*Beijing University of Posts and Telecommunications*),
Haixin Duan (*Tsinghua University & Quancheng Laboratory*)
- **Inbox Invasion: Exploiting MIME Ambiguities to Evade Email Attachment Detectors** 467
Jiahe Zhang (*Tsinghua University*), Jianjun Chen (*Tsinghua University & Zhongguancun Laboratory*),
Qi Wang (*Tsinghua University*), Hangyu Zhang (*Tsinghua University*), Chuhan Wang (*Tsinghua University*),
Jianwei Zhuze (*Tsinghua University & Zhongguancun Laboratory*),
Haixin Duan (*Tsinghua University & Zhongguancun Laboratory*)
- **Toward Understanding the Security of Plugins in Continuous Integration Services** 482
Xiaofan Li (*The University of Delaware*), Yacong Gu (*Tsinghua University QI-ANXIN Group*),
Chu Qiao (*The University of Delaware*), Zhenkai Zhang (*Clemson University*), Daiping Liu (*Palo Alto Networks*),
Lingyun Ying (*QI-ANXIN Technology Research Institute*),
Haixin Duan (*Tsinghua University Zhongguancun Laboratory*), Xing Gao (*The University of Delaware*)
- **The Harder You Try, The Harder You Fail: The KeyTrap Denial-of-Service Algorithmic Complexity Attacks on DNSSEC** 497
Elias Heftrig (*Fraunhofer SIT, ATHENE*), Haya Schulmann (*Goethe Uni Frankfurt, ATHENE*),
Niklas Vogel (*Goethe Uni Frankfurt, ATHENE*), Michael Waidner (*Fraunhofer SIT, Fraunhofer SIT, ATHENE*)

Session 2-2: Web Security I

- **FuzzCache: Optimizing Web Application Fuzzing Through Software-Based Data Cache.....** 511
Penghui Li (*Zhongguancun Laboratory*),
Mingxue Zhang (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*)
- **MiniCAT: Understanding and Detecting Cross-Page Request Forgery Vulnerabilities in Mini-Programs** 525
Zidong Zhang (*School of Cyber Science and Technology, Shandong University*),
Qinsheng Hou (*Shandong University; QI-ANXIN Technology Research Institute*),
Lingyun Ying (*QI-ANXIN Technology Research Institute*),
Wenrui Diao (*School of Cyber Science and Technology, Shandong University*),
Yacong Gu (*Tsinghua University; Tsinghua University-QI-ANXIN Group JCNS*),
Rui Li (*School of Cyber Science and Technology, Shandong University*),
Shanqing Guo (*School of Cyber Science and Technology, Shandong University*),
Haixin Duan (*Tsinghua University; Quancheng Laboratory*)
- **SWIDE: A Semantic-aware Detection Engine for Successful Web Injection Attacks** 540
Ronghai Yang (*Sangfor Technologies Inc.*), Xianbo Wang (*The Chinese University of Hong Kong*),
Kaixuan Luo (*The Chinese University of Hong Kong*), Xin Lei (*Sangfor Technologies Inc.*),
Ke Li (*Sangfor Technologies Inc.*), Jiayuan Xin (*Sangfor Technologies Inc.*),
Wing Cheong Lau (*The Chinese University of Hong Kong*)
- **Stealing Trust: Unraveling Blind Message Attacks in Web3 Authentication** 555
Kailun Yan (*School of Cyber Science and Technology, Shandong University*),
Xiaokuan Zhang (*Department of Computer Science, George Mason University*),
Wenrui Diao (*School of Cyber Science and Technology, Shandong University*)
- **Test Suites Guided Vulnerability Validation for Node.js Applications** 570
Changhua Luo (*Wuhan University & The Chinese University of Hong Kong*),
Penghui Li (*Zhongguancun Laboratory*), Wei Meng (*The Chinese University of Hong Kong*),
Chao Zhang (*Tsinghua University*)
- **ReactAppScan: Mining React Application Vulnerabilities via Component Graph** 585
Zhiyong Guo (*Johns Hopkins University*), Mingqing Kang (*Johns Hopkins University*),
V.N. Venkatakrishnan (*University of Illinois Chicago*), Rigel Gjormemo (*University of Illinois Chicago*),
Yinzhi Cao (*Johns Hopkins University*)

Session 2-3: ML and Security: Machine Learning Attacks

- **Certifiable Black-Box Attacks with Randomized Adversarial Examples: Breaking Defenses with Provable Confidence** 600
Hanbin Hong (*University of Connecticut*), Xinyu Zhang (*Zhejiang University*),
Binghui Wang (*Illinois Institute of Technology*), Zhongjie Ba (*Zhejiang University*),
Yuan Hong (*University of Connecticut*)
- **Phantom: Untargeted Poisoning Attacks on Semi-Supervised Learning** 615
Jonathan Knauer (*Technical University of Darmstadt*), Phillip Rieger (*Technical University of Darmstadt*),
Hossein Fereidooni (*KOBIL GmbH*), Ahmad-Reza Sadeghi (*Technical University of Darmstadt*)
- **Zero-Query Adversarial Attack on Black-box Automatic Speech Recognition Systems** 630
Zheng Fang (*Wuhan University*), Tao Wang (*Wuhan University*), Lingchen Zhao (*Wuhan University*),
Shenyi Zhang (*Wuhan University*), Bowen Li (*Wuhan University*), Yunjie Ge (*Wuhan University*),
Qi Li (*Tsinghua University*), Chao Shen (*Xi'an Jiaotong University*), Qian Wang (*Wuhan University*)
- **SUB-PLAY: Adversarial Policies against Partially Observed Multi-Agent Reinforcement Learning Systems** 645
Oubo Ma (*Zhejiang University*), Yuwen Pu (*Zhejiang University*), Linkang Du (*Xi'an Jiaotong University*),
Yang Dai (*Laboratory for Big Data and Decision*), Ruowang Wang (*Chinese Aeronautical Establishment*),
Xiaolei Liu (*Institute of Computer Application, China Academy of Engineering Physics*),
Yingcai Wu (*Zhejiang University*), Shouling Ji (*Zhejiang University*)
- **Optimization-based Prompt Injection Attack to LLM-as-a-Judge** 660
Jiawen Shi (*Huazhong University of Science and Technology*),
Zenghui Yuan (*Huazhong University of Science and Technology*),
Yinuo Liu (*Huazhong University of Science and Technology*), Yue Huang (*University of Notre Dame*),
Pan Zhou (*Huazhong University of Science and Technology*), Lichao Sun (*Lehigh University*),
Neil Zhenqiang Gong (*Duke University*)

- **NEURAL DEHYDRATION: Effective Erasure of Black-box Watermarks from DNNs with Limited Data**..... 675
Yifan Lu (*Fudan University*), Wenxuan Li (*Fudan University*), Mi Zhang (*Fudan University*),
Xudong Pan (*Fudan University*), Min Yang (*Fudan University*)

Session 2-4: Software Security: Fuzzing I

- **DarthShader: Fuzzing WebGPU Shader Translators & Compilers** 690
Lukas Bernhard (*CISPA Helmholtz Center for Information Security*),
Nico Schiller (*CISPA Helmholtz Center for Information Security*),
Moritz Schloegel (*CISPA Helmholtz Center for Information Security*),
Nils Bars (*CISPA Helmholtz Center for Information Security*),
Thorsten Holz (*CISPA Helmholtz Center for Information Security*)
- **OSMART: Whitebox Program Option Fuzzing**..... 705
Kelin Wang (*TCA, Institute of Software, Chinese Academy of Sciences & Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University*),
Mengda Chen (*TCA, Institute of Software, Chinese Academy of Sciences*),
Liang He (*TCA, Institute of Software, Chinese Academy of Sciences*),
Purui Su (*TCA, Institute of Software, Chinese Academy of Sciences & Key Laboratory of System Software (Chinese Academy of Sciences) and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences*),
Yan Cai (*Key Laboratory of System Software (Chinese Academy of Sciences) and State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences*),
Jiongyi Chen (*College of Electronic Science and Technology, National University of Defense Technology*),
Bin Zhang (*College of Electronic Science and Technology, National University of Defense Technology*),
Chao Feng (*College of Electronic Science and Technology, National University of Defense Technology*),
Chaojing Tang (*College of Electronic Science and Technology, National University of Defense Technology*)
- **Program Environment Fuzzing**..... 720
Ruijie Meng (*National University of Singapore*), Gregory J. Duck (*National University of Singapore*),
Abhik Roychoudhury (*National University of Singapore*)
- **ProphetFuzz: Fully Automated Prediction and Fuzzing of High-Risk Option Combinations with Only Documentation via Large Language Model** 735
Dawei Wang (*Zhongguancun Laboratory*), Geng Zhou (*Zhongguancun Laboratory*), Li Chen (*Zhongguancun Laboratory*), Dan Li (*Tsinghua University*), Yukai Miao (*Zhongguancun Laboratory*)
- **No Peer, no Cry: Network Application Fuzzing via Fault Injection** 750
Nils Bars (*CISPA Helmholtz Center for Information Security*),
Moritz Schloegel (*CISPA Helmholtz Center for Information Security*),
Nico Schiller (*CISPA Helmholtz Center for Information Security*),
Lukas Bernhard (*CISPA Helmholtz Center for Information Security*),
Thorsten Holz (*CISPA Helmholtz Center for Information Security*)
- **FOX: Coverage-guided Fuzzing as Online Stochastic Control** 765
Dongdong She (*Hong Kong University of Science and Technology*), Adam Storek (*Columbia University*),
Yuchong Xie (*Hong Kong University of Science and Technology*), Seoyoung Kweon (*Columbia University*),
Prashast Srivastava (*Columbia University*), Suman Jana (*Columbia University*)

Session 2-5: Applied Crypto: MPC I

- **Leakage-Resilient Circuit Garbling**..... 780
Ruiyang Li (*School of Cyber Science and Technology, Shandong University*),
Yiteng Sun (*School of Cyber Science and Technology, Shandong University*),
Chun Guo (*School of Cyber Science and Technology, Shandong University*),
François-Xavier Standaert (*ICTEAM/ELEN/Crypto Group, UCL*),
Weijia Wang (*School of Cyber Science and Technology, Shandong University*),
Xiao Wang (*Northwestern University*)
- **Secure Multiparty Computation with Lazy Sharing** 795
Shuaishuai Li (*Zhongguancun Laboratory*),
Cong Zhang (*Institute for Advanced Study, BNRist, Tsinghua University*),
Dongdai Lin (*Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, Chinese Academy of Sciences & School of Cyber Security, University of Chinese Academy of Sciences*)

- **Coral: Maliciously Secure Computation Framework for Packed and Mixed Circuits** 810
Zhicong Huang (*Ant Group*), Wen-jie Lu (*Ant Group & Zhejiang University*), Yuchen Wang (*Ant Group*),
Cheng Hong (*Ant Group*), Tao Wei (*Ant Group*), WenGuang Chen (*Ant Group*)
- **Sublinear Distributed Product Checks on Replicated Secret-Shared Data over \mathbb{Z}_2^k Without Ring Extensions** 825
Yun Li (*Ant Group*), Daniel Escudero (*J.P. Morgan AI Research & J.P. Morgan AlgoCRYPT CoE*),
Yufei Duan (*Tsinghua University*), Zhicong Huang (*Ant Group*), Cheng Hong (*Ant Group*),
Chao Zhang (*Tsinghua University*), Yifan Song (*Tsinghua University & Shanghai Qi Zhi Institute*)
- **Secret Sharing with Snitching** 840
Stefan Dziembowski (*University of Warsaw & IDEAS NCBR*), Sebastian Faust (*Technische Universität Darmstadt*),
Tomasz Lazurek (*University of Warsaw & NASK*), Marcin Mieleniczuk (*University of Warsaw*)
- **SHORTCUT: Making MPC-based Collaborative Analytics Efficient on Dynamic Databases** 854
Peizhao Zhou (*CS, DISec, Nankai University*),
Xiaojie Guo (*CS, DISec, Nankai University & Shanghai Qi Zhi Institute*),
Pinzhi Chen (*CS, DISec, Nankai University*), Tong Li (*CS, DISec, Nankai University*),
Siyi Lv (*CS, DISec, Nankai University*), Zheli Liu (*CS, DISec, Nankai University*)

Session 2-6: Applied Crypto: Zero Knowledge Proofs I

- **Dora: A Simple Approach to Zero-Knowledge for RAM Programs** 869
Aarushi Goel (*Purdue University*), Mathias Hall-Andersen (*Aarhus University & Galois*),
Gabriel Kaptchuk (*University of Maryland*)
- **Dual Polynomial Commitment Schemes and Applications to Commit-and-Prove SNARKs** .. 884
Chaya Ganesh (*Indian Institute of Science*), Vineet Nair (*Arithmetic Labs*), Ashish Sharma (*Arithmetic Labs*)
- **Direct Range Proofs for Paillier Cryptosystem and Their Applications** 899
Zhikang Xie (*The University of Hong Kong*), Mengling Liu (*The Hong Kong Polytechnic University*),
Haiyang Xue (*Singapore Management University*), Man Ho Au (*The Hong Kong Polytechnic University*),
Robert H. Deng (*Singapore Management University*), Siu-Ming Yiu (*The University of Hong Kong*)
- **CONAN: Distributed Proofs of Compliance for Anonymous Data Collection** 914
Mingxun Zhou (*Carnegie Mellon University & IC3*), Giulia Fanti (*Carnegie Mellon University & IC3*),
Elaine Shi (*Carnegie Mellon University*)
- **HEKATON: Horizontally-Scalable zkSNARKs Via Proof Aggregation** 929
Michael Rosenberg (*University of Maryland*), Tushar Mopuri (*University of Pennsylvania*), Hossein Hafezi (*New York University*), Ian Miers (*University of Maryland*), Pratyush Mishra (*University of Pennsylvania*)
- **GRLandLine: Adaptively Secure DKG and Randomness Beacon with (Log-)Quadratic Communication Complexity** 941
Renas Bacho (*CISPA Helmholtz Center for Information Security & Saarland University*),
Christoph Lenzen (*CISPA Helmholtz Center for Information Security*),
Julian Loss (*CISPA Helmholtz Center for Information Security*),
Simon Ochsenreither (*Vector Informatik GmbH*), Dimitrios Papachristoudis (*Researcher*)

Session 2-7: Blockchain & Distributed Systems: Blockchain Attacks

- **TOKENSCOUT: Early Detection of Ethereum Scam Tokens via Temporal Graph Learning** 956
Cong Wu (*Nanyang Technological University*), Jing Chen (*Wuhan University*),
Ziming Zhao (*Northeastern University*), Kun He (*Wuhan University*),
Guowen Xu (*University of Electronic Science and Technology of China*),
Yueming Wu (*Nanyang Technological University*), Haijun Wang (*Xi'an Jiaotong University*),
Hongwei Li (*University of Electronic Science and Technology of China*),
Yang Liu (*Nanyang Technological University*), Yang Xiang (*Swinburne University of Technology*)
- **FAMULET: Finding Finalization Failure Bugs in Polygon zkRollup** 971
Zihao Li (*The Hong Kong Polytechnic University*), Xinghao Peng (*The Hong Kong Polytechnic University*),
Zheyuan He (*University of Electronic Science and Technology of China*),
Xiapu Luo (*The Hong Kong Polytechnic University*),
Ting Chen (*University of Electronic Science and Technology of China*)
- **Characterizing Ethereum Address Poisoning Attack** 986
Shixuan Guan (*San Diego State University*), Kai Li (*San Diego State University*)

- **FORAY: Towards Effective Attack Synthesis against Deep Logical Vulnerabilities in DeFi Protocols**..... 1001
Hongbo Wen (*University of California, Santa Barbara*), Hanzhi Liu (*University of California, Santa Barbara*), Jiaxin Song (*University of Illinois Urbana-Champaign*), Yanju Chen (*University of California, Santa Barbara*), Wenbo Guo (*University of California, Santa Barbara*), Yu Feng (*University of California, Santa Barbara*)
- **Towards Automatic Discovery of Denial of Service Weaknesses in Blockchain Resource Models**..... 1016
Feng Luo (*The Hong Kong Polytechnic University & University of Electronic Science and Technology of China*), Huangkun Lin (*University of Electronic Science and Technology of China*), Zihao Li (*The Hong Kong Polytechnic University*), Xiapu Luo (*The Hong Kong Polytechnic University*), Ruijie Luo (*University of Electronic Science and Technology of China*), Zheyuan He (*University of Electronic Science and Technology of China*), Shuwei Song (*University of Electronic Science and Technology of China*), Ting Chen (*University of Electronic Science and Technology of China*), Wenxuan Luo (*University of Electronic Science and Technology of China*)
- **Blockchain Bribing Attacks and the Efficacy of Counterincentives**..... 1031
Dimitris Karakostas (*University of Edinburgh*), Aggelos Kiayias (*University of Edinburgh & IOG*), Thomas Zacharias (*University of Glasgow*)

Session 3-1: Formal Methods and Programming Languages I

- **Keeping Up with the KEMs: Stronger Security Notions for KEMs and Automated Analysis of KEM-based Protocols** 1046
Cas Cremers (*CISPA Helmholtz Center for Information Security*), Alexander Dax (*CISPA Helmholtz Center for Information Security*), Niklas Medinger (*CISPA Helmholtz Center for Information Security*)
- **SECOMP: Formally Secure Compilation of Compartmentalized C Programs** 1061
Jérémy Thibault (*Max Planck Institute for Security and Privacy (MPI-SP)*), Roberto Blanco (*Max Planck Institute for Security and Privacy (MPI-SP)*), Dongjae Lee (*Seoul National University*), Sven Argo (*Ruhr University Bochum*), Arthur Azevedo de Amorim (*Rochester Institute of Technology*), Aina Linn Georges (*Max Planck Institute for Software Systems (MPI-SWS)*), Cătălin Hrițcu (*Max Planck Institute for Security and Privacy (MPI-SP)*), Andrew Tolmach (*Portland State University*)
- **Testing Side-channel Security of Cryptographic Implementations against Future Microarchitectures**..... 1076
Gilles Barthe (*Max Planck Institute for Security and Privacy & IMDEA Software Institute*), Marcel Böhme (*Max Planck Institute for Security and Privacy*), Sunjay Cauligi (*Max Planck Institute for Security and Privacy*), Chitchanok Chuengsatansup (*The University of Melbourne*), Daniel Genkin (*Georgia Tech*), Marco Guarnieri (*IMDEA Software Institute*), David Mateos Romero (*IMDEA Software Institute*), Peter Schwabe (*Max Planck Institute for Security and Privacy & Radboud University*), David Wu (*University of Adelaide*), Yuval Yarom (*Ruhr University Bochum*)
- **On Kernel's Safety in the Spectre Era (And KASLR is Formally Dead)** 1091
Davide Davoli (*Inria, Université Côte d'Azur*), Martin Avanzini (*Inria, Université Côte d'Azur*), Tamara Rezk (*Inria, Université Côte d'Azur*)
- **The Privacy-Utility Trade-off in the Topics API** 1106
Mário S. Alvim (*Universidade Federal de Minas Gerais*), Natasha Fernandes (*Macquarie University*), Annabelle McIver (*Macquarie University*), Gabriel H. Nunes (*Macquarie University & Universidade Federal de Minas Gerais*)
- **Specification and Verification of Strong Timing Isolation of Hardware Enclaves**..... 1121
Stella Lau (*Massachusetts Institute of Technology*), Thomas Bourgeat (*EPFL*), Clément Pit-Claudel (*EPFL*), Adam Chlipala (*Massachusetts Institute of Technology*)

Session 3-2: ML and Security: Large Language Models

- **A Causal Explainable Guardrails for Large Language Models**..... 1136
Zhixuan Chu (*Zhejiang University & State Key Laboratory of Blockchain and Data Security*), Yan Wang (*Ant Group*), Longfei Li (*Ant Group*), Zhibo Wang (*Zhejiang University*), Zhan Qin (*Zhejiang University*), Kui Ren (*Zhejiang University*)

- **LEGILIMENS: Practical and Unified Content Moderation for Large Language Model Services....**1151
Jialin Wu (*Zhejiang University*), Jiangyi Deng (*Zhejiang University*), Shengyuan Pang (*Zhejiang University*), Yanjiao Chen (*Zhejiang University*), Jiayang Xu (*Zhejiang University*), Xinfeng Li (*Zhejiang University*), Wenyan Xu (*Zhejiang University*)
- **SurrogatePrompt: Bypassing the Safety Filter of Text-to-Image Models via Substitution.....** 1166
Zhongjie Ba (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*), Jieming Zhong (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*), Jiachen Lei (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*), Peng Cheng (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*), Qinglong Wang (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*), Zhan Qin (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*), Zhibo Wang (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*), Kui Ren (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*)
- **Moderator: Moderating Text-to-Image Diffusion Models through Fine-grained Context-based Policies** 1181
Peiran Wang (*Tsinghua University*), Qiyu Li (*University of California, San Diego*), Longxuan Yu (*University of California, San Diego*), Ziyao Wang (*University of Maryland College Park*), Ang Li (*University of Maryland College Park*), Haojian Jin (*University of California, San Diego*)
- **GenderCARE: A Comprehensive Framework for Assessing and Reducing Gender Bias in Large Language Models** 1196
Kunsheng Tang (*University of Science and Technology of China*), Wenbo Zhou (*University of Science and Technology of China*), Jie Zhang (*Nanyang Technological University*), Aishan Liu (*Beihang University*), Gelei Deng (*Nanyang Technological University*), Shuai Li (*University of Science and Technology of China*), Peigui Qi (*University of Science and Technology of China*), Weiming Zhang (*University of Science and Technology of China*), Tianwei Zhang (*Nanyang Technological University*), Nenghai Yu (*University of Science and Technology of China*)
- **Understanding Implosion in Text-to-Image Generative Models.....** 1211
Wenxin Ding (*University of Chicago*), Cathy Y. Li (*University of Chicago*), Shawn Shan (*University of Chicago*), Ben Y. Zhao (*University of Chicago*), Haitao Zheng (*University of Chicago*)

Session 3-3:ML and Security: Inference Attacks

- **Is Difficulty Calibration All We Need? Towards More Practical Membership Inference Attacks** 1226
Yu He (*Wuhan University*), Boheng Li (*Wuhan University*), Yao Wang (*Wuhan University*), Mengda Yang (*Wuhan University*), Juan Wang (*Wuhan University*), Hongxin Hu (*University at Buffalo*), Xingyu Zhao (*University of Warwick*)
- **A Unified Membership Inference Method for Visual Self-supervised Encoder via Part-aware Capability** 1241
Jie Zhu (*Key Lab of High Confidence Software Technologies (Peking University), Ministry of Education & School of Computer Science, Peking University*), Jirong Zha (*Tsinghua-Berkeley Shenzhen Institute, Tsinghua University*), Ding Li (*Key Lab of High Confidence Software Technologies (Peking University), Ministry of Education & School of Computer Science, Peking University*), Leye Wang (*Key Lab of High Confidence Software Technologies (Peking University), Ministry of Education & School of Computer Science, Peking University*)
- **Membership Inference Attacks against Vision Transformers: Mosaic MixUp Training to the Defense** 1256
Qiankun Zhang (*School of Cyber Science and Engineering, Huazhong University of Science and Technology*), Di Yuan (*School of Cyber Science and Engineering, Huazhong University of Science and Technology*), Boyu Zhang (*School of Cyber Science and Engineering, Huazhong University of Science and Technology*), Bin Yuan (*School of Cyber Science and Engineering, Huazhong University of Science and Technology*), Bingqian Du (*School of Computer Science and Technology, Huazhong University of Science and Technology*)
- **Evaluations of Machine Learning Privacy Defenses are Misleading** 1271
Michael Aerni (*ETH Zurich*), Jie Zhang (*ETH Zurich*), Florian Tramèr (*ETH Zurich*)

- **The Janus Interface: How Fine-Tuning in Large Language Models Amplifies the Privacy Risks** 1285
Xiaoyi Chen (*Indiana University Bloomington*), Siyuan Tang (*Indiana University Bloomington*), Rui Zhu (*Indiana University Bloomington*), Shijun Yan (*JD Cloud*), Lei Jin (*JD Cloud*), Zihao Wang (*Indiana University Bloomington*), Liya Su (*JD Cloud*), Zhikun Zhang (*Zhejiang University*), XiaoFeng Wang (*Indiana University Bloomington*), Haixu Tang (*Indiana University Bloomington*)
- **A General Framework for Data-Use Auditing of ML Models**..... 1300
Zonghao Huang (*Duke University*), Neil Zhenqiang Gong (*Duke University*), Michael K. Reiter (*Duke University*)

Session 3-4: Software Security: Memory Safety and Error Detection

- **COUNTDOWN: Refcount-guided Fuzzing for Exposing Temporal Memory Errors in Linux Kernel** 1315
Shuangpeng Bai (*The Pennsylvania State University*), Zhechang Zhang (*The Pennsylvania State University*), Hong Hu (*The Pennsylvania State University*)
- **Top of the Heap: Efficient Memory Error Protection of Safe Heap Objects**..... 1330
Kaiming Huang (*The Pennsylvania State University*), Mathias Payer (*École Polytechnique Fédérale de Lausanne*), Zhiyun Qian (*University of California, Riverside*), Jack Sampson (*The Pennsylvania State University*), Gang Tan (*The Pennsylvania State University*), Trent Jaeger (*University of California, Riverside*)
- **Safeslab: Mitigating Use-After-Free Vulnerabilities via Memory Protection Keys** 1345
Marius Momeu (*Technical University of Munich & Brown University*), Simon Schnücker (*Technical University of Munich*), Kai Angris (*Technical University of Munich*), Michalis Polychronakis (*Stony Brook University*), Vasileios P. Kemerlis (*Brown University*)
- **The Illusion of Randomness: An Empirical Analysis of Address Space Layout Randomization Implementations** 1360
Lorenzo Binosi (*Politecnico di Milano*), Gregorio Barzasi (*Politecnico di Milano*), Michele Carminati (*Politecnico di Milano*), Stefano Zanero (*Politecnico di Milano*), Mario Polino (*Politecnico di Milano*)
- **SEMALLOC: Semantics-Informed Memory Allocator** 1375
Ruizhe Wang (*University of Waterloo*), Meng Xu (*University of Waterloo*), N. Asokan (*University of Waterloo*)
- **Crossing Shifted Moats: Replacing Old Bridges with New Tunnels to Confidential Containers**..... 1390
Enriquillo Valdez (*IBM Research*), Salman Ahmed (*IBM Research*), Zhongshu Gu (*IBM Research*), Christophe de Dinechin (*Red Hat*), Pau-Chen Cheng (*IBM Research*), Hani Jamjoom (*IBM Research*)

Session 3-5: Applied Crypto: Private Information Retrieval & Private Set operations

- **Faster FHE-Based Single-Server Private Information Retrieval** 1405
Ming Luo (*Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS & School of Cyber Security, University of Chinese Academy of Sciences*), Feng-Hao Liu (*Washington State University*), Han Wang (*Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS & School of Cyber Security, University of Chinese Academy of Sciences*)
- **Simple and Practical Amortized Sublinear Private Information Retrieval using Dummy Subsets** 1420
Ling Ren (*University of Illinois at Urbana-Champaign*), Muhammad Haris Mughees (*University of Illinois at Urbana-Champaign*), I Sun (*University of Illinois at Urbana-Champaign*)
- **Unbalanced Private Set Union with Reduced Computation and Communication** 1434
Cong Zhang (*Institute for Advanced Study, BNRist, Tsinghua University*), Yu Chen (*School of Cyber Science and Technology, Shandong University & Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University*), Weiran Liu (*Alibaba Group*), Liqiang Peng (*Alibaba Group*), Meng Hao (*Singapore Management University*), Anyu Wang (*Institute for Advanced Study, BNRist, Tsinghua University & Zhongguancun Laboratory*), Xiaoyun Wang (*Institute for Advanced Study, BNRist, Tsinghua University & School of Cyber Science and Technology, Shandong University*)

- **ThorPIR: Single Server PIR via Homomorphic Thorp Shuffles** 1448
Ben Fisch (*Yale University*), Arthur Lazzaretti (*Yale University*), Zeyu Liu (*Yale University*), Charalampos Papamanthou (*Yale University*)
- **RESPIRE: High-Rate PIR for Databases with Small Records** 1463
Alexander Burton (*UT Austin*), Samir Jordan Menon (*Blyss*), David J. Wu (*UT Austin*)
- **Actively Secure Private Set Intersection in the Client-Server Setting** 1478
Yunqing Sun (*Northwestern University*), Jonathan Katz (*Google LLC & University of Maryland*), Mariana Raykova (*Google LLC*), Phillipp Schoppmann (*Google LLC*), Xiao Wang (*Northwestern University*)

Session 3-6: Applied Crypto: Signatures, Proofs, Integrity Schemes

- **Functional Adaptor Signatures: Beyond All-or-Nothing Blockchain-based Payments** 1493
Nikhil Vanjani (*Carnegie Mellon University*), Pratik Soni (*University of Utah*), Sri AravindaKrishnan Thyagarajan (*University of Sydney*)
- **Blind Multisignatures for Anonymous Tokens with Decentralized Issuance** 1508
Ioanna Karantaidou (*George Mason University & New York University*), Omar Renawi (*CISPA Helmholtz Center for Information Security & Saarland University*), Foteini Baldimtsi (*George Mason University & Mysten Labs*), Nikolaos Kamarinakis (*University of Maryland & Common Prefix*), Jonathan Katz (*Google & University of Maryland*), Julian Loss (*CISPA Helmholtz Center for Information Security*)
- **Practical Post-Quantum Signatures for Privacy** 1523
Sven Argo (*Faculty of Computer Science, HGI, Ruhr University Bochum*), Tim Güneysu (*Faculty of Computer Science, HGI, Ruhr University Bochum & Cyber Physical Systems, DFKI GmbH*), Corentin Jeudy (*Orange Labs, Applied Crypto Group & Univ Rennes, CNRS, IRISA*), Georg Land (*Faculty of Computer Science, HGI, Ruhr-University Bochum*), Adeline Roux-Langlois (*Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC*), Olivier Sanders (*Orange Labs*)
- **Reckle Trees: Updatable Merkle Batch Proofs with Applications** 1538
Charalampos Papamanthou (*Lagrange Labs & Yale University*), Shravan Srinivasan (*Lagrange Labs*), Nicolas Gailly (*Lagrange Labs*), Ismael Hishon-Rezaizadeh (*Lagrange Labs*), Andrus Salumets (*Lagrange Labs*), Stjepan Golemac (*Lagrange Labs*)
- **Provable Security for PKI Schemes** 1552
Sara Wrótniak (*School of Computing, University of Connecticut*), Hemi Leibowitz (*Faculty of Computer Science, The College of Management Academic Studies*), Ewa Syta (*Department of Computer Science, Trinity College*), Amir Herzberg (*School of Computing, University of Connecticut*)
- **Fast Two-party Threshold ECDSA with Proactive Security** 1567
Brian Koziel (*TripleBlind*), S. Dov Gordon (*TripleBlind & George Mason University*), Craig Gentry (*TripleBlind*)

Session 3-7: Usability and Measurement: Measuring and Understanding Privacy

- **Are We Getting Well-informed? An In-depth Study of Runtime Privacy Notice Practice in Mobile Apps** 1581
Shuai Li (*Fudan University*), Zheming Yang (*Fudan University*), Yuhong Nan (*Sun Yat-sen University*), Shutian Yu (*Fudan University*), Qirui Zhu (*Fudan University*), Min Yang (*Fudan University*)
- **Graphical vs. Deep Generative Models: Measuring the Impact of Differentially Private Mechanisms and Budgets on Utility** 1596
Georgi Ganev (*University College London and Hazy*), Kai Xu (*MIT-IBM Watson AI Lab*), Emiliano De Cristofaro (*University of California, Riverside*)
- **A Qualitative Analysis of Practical De-Identification Guides** 1611
Wentao Guo (*University of Maryland*), Aditya Kishore (*University of Maryland*), Adam J. Aviv (*The George Washington University*), Michelle L. Mazurek (*University of Maryland*)
- **A First Look at Security and Privacy Risks in the RapidAPI Ecosystem** 1626
Song Liao (*Texas Tech University*), Long Cheng (*Clemson University*), Xiapu Luo (*The Hong Kong Polytechnic University*), Zheng Song (*University of Michigan-Dearborn*), Haipeng Cai (*Washington State University*), Danfeng (Daphne) Yao (*Virginia Tech*), Hongxin Hu (*University at Buffalo*)

- **Measuring Compliance Implications of Third-party Libraries' Privacy Label Disclosure Guidelines** 1641
Yue Xiao (*Indiana University Bloomington*), Chaoqi Zhang (*Indiana University Bloomington*), Yue Qin (*Indiana University Bloomington*), Fares Fahad S Alharbi (*Indiana University Bloomington*), Luyi Xing (*Indiana University Bloomington*), Xiaojing Liao (*Indiana University Bloomington*)
- **Trust, Because You Can't Verify: Privacy and Security Hurdles in Education Technology Acquisition Practices** 1656
Easton Kelso (*Arizona State University*), Ananta Soneji (*Arizona State University*), S azzadur Rahaman (*University of Arizona*), Yan Shoshitaishvili (*Arizona State University*), Rakibul Hasan (*Arizona State University*)

Session 4-1: Usability and Measurement: Attack Measurements

- **"Do Anything Now": Characterizing and Evaluating In-The-Wild Jailbreak Prompts on Large Language Models** 1671
Xinyue Shen (*CISPA Helmholtz Center for Information Security*), Zeyuan Chen (*CISPA Helmholtz Center for Information Security*), Michael Backes (*CISPA Helmholtz Center for Information Security*), Yun Shen (*NetApp*), Yang Zhang (*CISPA Helmholtz Center for Information Security*)
- **Breaching Security Keys without Root: FIDO2 Deception Attacks via Overlays exploiting Limited Display Authenticators** 1686
Ahmed Tanvir Mahdad (*Texas A&M University*), Mohammed Jubur (*Jazan University*), Nitesh Saxena (*Texas A&M University*)
- **The Not-So-Silent Type: Vulnerabilities in Chinese IME Keyboards' Network Security Protocols** 1701
Jeffrey Knockel (*Citizen Lab, University of Toronto*), Mona Wang (*Princeton University*), Zoë Reichert (*Citizen Lab, University of Toronto*)
- **Demystifying RCE Vulnerabilities in LLM-Integrated Apps** 1716
Tong Liu (*IIIE, CAS & School of Cyber Security, UCAS*), Zizhuang Deng (*School of Cyber Science and Technology, Shandong University*), Guozhu Meng (*IIIE, CAS & School of Cyber Security, UCAS*), Yuekang Li (*University of New South Wales*), Kai Chen (*IIIE, CAS & School of Cyber Security, UCAS*)

Session 4-2: HW & CPS: Attacks and Defenses in Smart Devices

- **GAZEPOIT: Remote Keystroke Inference Attack by Gaze Estimation from Avatar Views in VR/MR Devices** 1731
Hanqiu Wang (*Department of Electrical and Computer Engineering, University of Florida*), Zihao Zhan (*Department of Computer Science, Texas Tech University*), Haoqi Shan (*CertiK*), Siqi Dai (*Department of Electrical and Computer Engineering, University of Florida*), Maximilian Panoff (*Department of Electrical and Computer Engineering, University of Florida*), Shuo Wang (*Department of Electrical and Computer Engineering, University of Florida*)
- **VPVet: Vetting Privacy Policies of Virtual Reality Apps** 1746
Yuxia Zhan (*Shanghai Jiao Tong University*), Yan Meng (*Shanghai Jiao Tong University*), Lu Zhou (*Xidian University*), Yichang Xiong (*George Mason University*), Xiaokuan Zhang (*George Mason University*), Lichuan Ma (*Xidian University*), Guoxing Chen (*Shanghai Jiao Tong University*), Qingqi Pei (*Xidian University*), Haojin Zhu (*Shanghai Jiao Tong University*)
- **Collapse Like A House of Cards: Hacking Building Automation System Through Fuzzing** .. 1761
Yue Zhang (*Drexel University*), Zhen Ling (*Southeast University*), Michael Cash (*University of Central Florida*), Qiguang Zhang (*Southeast University*), Christopher Morales-Gonzalez (*UMass Lowell*), Qun Zhou Sun (*University of Central Florida*), Xinwen Fu (*UMass Lowell*)
- **Watch the Rhythm: Breaking Privacy with Accelerometer at the Extremely-Low Sampling Rate of 5Hz** 1776
Qingsong Yao (*State Key Lab of ISN, School of Cyber Engineering, Xidian University*), Yuming Liu (*State Key Lab of ISN, School of Cyber Engineering, Xidian University*), Xiongjia Sun (*State Key Lab of ISN, School of Cyber Engineering, Xidian University*), Xuewen Dong (*School of Computer Science and Technology, Xidian University*), Xiaoyu Ji (*Department of Electrical Engineering, Zhejiang University*), Jianfeng Ma (*State Key Lab of ISN, School of Cyber Engineering, Xidian University*)

Session 4-3: Privacy and Anonymity & Applied Crypto: Privacy and Systems

- **CAPSID: A Private Session ID System for Small UAVs** 1791
Yueshen Li (*University of Illinois at Urbana-Champaign*), Jianli Jin (*University of Illinois at Urbana-Champaign*), Kirill Levchenko (*Electrical and Computer Engineering, University of Illinois at Urbana-Champaign*)
- **MaskPrint: Take the Initiative in Fingerprint Protection to Mitigate the Harm of Data Breach** 1806
Yihui Yan (*School of Information Science and Technology, ShanghaiTech University*), Zhice Yang (*School of Information Science and Technology, ShanghaiTech University*)
- **Precio: Private Aggregate Measurement via Oblivious Shuffling**..... 1819
Erik Anderson (*Microsoft*), Melissa Chase (*Microsoft Research*), F. Betül Durak (*Microsoft Research*), Kim Laine (*Microsoft Research*), Chenkai Weng (*Northwestern University*)
- **Formal Privacy Proof of Data Encoding: The Possibility and Impossibility of Learnable Encryption** 1834
Hanshen Xiao (*Purdue University/NVIDIA Research*), G. Edward Suh (*NVIDIA Research/Cornell University*), Srinivas Devadas (*Massachusetts Institute of Technology*)

Session 4-4: HW & CPS: Security of Autonomous Vehicles

- **SpecGuard: Specification Aware Recovery for Robotic Autonomous Vehicles from Physical Attacks**..... 1849
Pritam Dash (*University of British Columbia*), Ethan Chan (*University of British Columbia*), Karthik Pattabiraman (*University of British Columbia*)
- **VisionGuard: Secure and Robust Visual Perception of Autonomous Vehicles in Practice** 1864
Xingshuo Han (*Nanyang Technological University*), Haozhao Wang (*Huazhong University of Science and Technology*), Kangqiao Zhao (*Nanyang Technological University*), Gelei Deng (*Nanyang Technological University*), Yuan Xu (*Nanyang Technological University*), Hangcheng Liu (*Nanyang Technological University*), Han Qiu (*Tsinghua University*), Tianwei Zhang (*Nanyang Technological University*)
- **PhyScout: Detecting Sensor Spoofing Attacks via Spatio-temporal Consistency** 1879
Yuan Xu (*College of Computing and Data Science, Nanyang Technological University*), Gelei Deng (*College of Computing and Data Science, Nanyang Technological University*), Xingshuo Han (*College of Computing and Data Science, Nanyang Technological University*), Guanlin Li (*College of Computing and Data Science, Nanyang Technological University*), Han Qiu (*Institute for Network Sciences and Cyberspace, Tsinghua University*), Tianwei Zhang (*College of Computing and Data Science, Nanyang Technological University*)
- **ERACAN: Defending Against an Emerging CAN Threat Model**..... 1894
Zhaozhou Tang (*Georgia Institute of Technology*), Khaled Serag (*Qatar Computing Research Institute*), Saman Zonouz (*Georgia Institute of Technology*), Z. Berkay Celik (*Purdue University*), Dongyan Xu (*Purdue University*), Raheem Beyah (*Georgia Institute of Technology*)

Session 4-5: Privacy and Anonymity: Differential Privacy II

- **Elephants Do Not Forget: Differential Privacy with State Continuity for Privacy Budget** 1909
Jiankai Jin (*The University of Melbourne*), Chitchanok Chuengsatiansup (*The University of Melbourne*), Toby Murray (*The University of Melbourne*), Benjamin I. P. Rubinstein (*The University of Melbourne*), Yuval Yarom (*Ruhr University Bochum*), Olga Ohrimenko (*The University of Melbourne*)
- **ProBE: Proportioning Privacy Budget for Complex Exploratory Decision Support** 1924
Nada Lahjouji (*University of California, Irvine*), Sameera Ghayyur (*Snap Inc.*), Xi He (*University of Waterloo*), Sharad Mehrotra (*University of California, Irvine*)
- **Almost Instance-optimal Clipping for Summation Problems in the Shuffle Model of Differential Privacy** 1939
Wei Dong (*Nanyang Technological University*), Qiyao Luo (*OceanBase, Ant Group*), Giulia Fanti (*Carnegie Mellon University*), Elaine Shi (*Carnegie Mellon University*), Ke Yi (*Hong Kong University of Science and Technology*)
- **Securing Floating-Point Arithmetic for Noise Addition**..... 1954
Naoise Holohan (*IBM Research Europe -- Ireland*), Stefano Braghin (*IBM Research Europe -- Ireland*), Mohamed Suliman (*IBM Research Europe -- Ireland & Trinity College Dublin*)

Session 4-6: Privacy and Anonymity: Anonymous Communication

- **Distributed PIR: Scaling Private Messaging via the Users' Machines** 1967
Elkana Tovey (*Hebrew University*), Jonathan Weiss (*Hebrew University*), Yossi Gilad (*Hebrew University*)
- **Bytes to Schlep? Use a FEP: Hiding Protocol Metadata with Fully Encrypted Protocols** 1982
Ellis Fenske (*U.S. Naval Academy*), Aaron Johnson (*U.S. Naval Research Laboratory*)
- **Robust and Reliable Early-Stage Website Fingerprinting Attacks via Spatial-Temporal Distribution Analysis** 1997
Xinhao Deng (*INSC & BNRist, Tsinghua University*),
Qi Li (*INSC, Tsinghua University & Zhongguancun Laboratory*),
Ke Xu (*DCST, Tsinghua University & Zhongguancun Laboratory*)
- **HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted** 2012
Yanxue Jia (*Purdue University*), Varun Madathil (*North Carolina State University*),
Aniket Kate (*Purdue University / Supra Research*)

Session 5-1: Network Security: Wireless Networks

- **RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces**. 2027
Nathaniel Bennett (*University of Florida*), Weidong Zhu (*University of Florida*),
Benjamin Simon (*University of Florida*), Ryon Kennedy (*University of Florida*),
William Enck (*North Carolina State University*), Patrick Traynor (*University of Florida*),
Kevin R. B. Butler (*University of Florida*)
- **Jäger: Automated Telephone Call Traceback** 2042
David Adei (*North Carolina State University*), Varun Madathil (*North Carolina State University*),
Sathvik Prasad (*North Carolina State University*), Bradley Reaves (*North Carolina State University*),
Alessandra Scafuro (*North Carolina State University*)
- **Strong Privacy-Preserving Universally Composable AKA Protocol with Seamless Handover Support for Mobile Virtual Network Operator** 2057
Rabiah Alnashwan (*The University of Sheffield*), Yang Yang (*National University of Singapore*),
Yilu Dong (*The Pennsylvania State University*), Prosanta Gope (*The University of Sheffield*),
Behzad Abdolmaleki (*The University of Sheffield*), Syed Rafiul Hussain (*The Pennsylvania State University*)
- **Untangling the Knot: Breaking Access Control in Home Wireless Mesh Networks** 2072
Xin'an Zhou (*University of California, Riverside*), Qing Deng (*University of California, Riverside*),
Juefei Pu (*University of California, Riverside*), Keyu Man (*University of California, Riverside*),
Zhiyun Qian (*University of California, Riverside*), Srikanth V. Krishnamurthy (*University of California, Riverside*)
- **BlueSWAT: A Lightweight State-Aware Security Framework for Bluetooth Low Energy** 2087
Xijia Che (*INSC & BNRist, Tsinghua University*), Yi He (*INSC, Tsinghua University*),
Xuewei Feng (*DCS, Tsinghua University*), Kun Sun (*IST, George Mason University*),
Ke Xu (*DCS, Tsinghua University & Zhongguancun Laboratory*),
Qi Li (*INSC, Tsinghua University & Zhongguancun Laboratory*)
- **State Machine Mutation-based Testing Framework for Wireless Communication Protocols** 2102
Syed Md Mukit Rashid (*The Pennsylvania State University*), Tianwei Wu (*The Pennsylvania State University*),
Kai Tu (*The Pennsylvania State University*), Abdullah Al Ishtiaq (*The Pennsylvania State University*),
Ridwanul Hasan Tanvir (*The Pennsylvania State University*), Yilu Dong (*The Pennsylvania State University*),
Omar Chowdhury (*Stony Brook University*), Syed Rafiul Hussain (*The Pennsylvania State University*)

Session 5-2: Web Security II

- **Peeking through the window: Fingerprinting Browser Extensions through Page-Visible Execution Traces and Interactions** 2117
Shubham Agarwal (*CISPA Helmholtz Center for Information Security*),
Aurore Fass (*CISPA Helmholtz Center for Information Security*),
Ben Stock (*CISPA Helmholtz Center for Information Security*)
- **Understanding Cross-Platform Referral Traffic for Illicit Drug Promotion** 2132
Mingming Zha (*Indiana University Bloomington*), Zilong Lin (*Indiana University Bloomington*),
Siyuan Tang (*Indiana University Bloomington*), Xiaojing Liao (*Indiana University Bloomington*),
Yuhong Nan (*Sun Yat-sen University*), XiaoFeng Wang (*Indiana University Bloomington*)

- **Characterizing and Mitigating Phishing Attacks at ccTLD Scale**..... 2147
Giovane C. M. Moura (*SIDN Labs & Delft University of Technology*),
Thomas Daniels (*DNS Belgium & Department of Computer Science, KU Leuven*),
Maarten Bosteels (*DNS Belgium*), Sebastian Castro (*.IE Registry*),
Moritz Müller (*SIDN Labs & University of Twente*), Thymen Wabeke (*SIDN Labs*),
Thijs van den Hout (*SIDN Labs*), Maciej Korczyński (*Univ. Grenoble Alps*),
Georgios Smaragdakis (*Delft University of Technology*)
- **The Big Brother’s New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User’s Perspective** 2162
Andrea Mengascini (*CISPA Helmholtz Center for Information Security*),
Ryan Aurelio (*CISPA Helmholtz Center for Information Security*),
Giancarlo Pellegrino (*CISPA Helmholtz Center for Information Security*)
- **Blocking Tracking JavaScript at the Function Granularity** 2177
Abdul Haddi Amjad (*Virginia Tech*), Shaoor Munir (*University of California*),
Zubair Shafiq (*University of California*), Muhammad Ali Gulzar (*Virginia Tech*)
- **Unbundle-Rewrite-Rebundle: Runtime Detection and Rewriting of Privacy-Harming Code in JavaScript Bundles**..... 2192
Mir Masood Ali (*University of Illinois Chicago*), Peter Snyder (*Brave Software*),
Chris Kanich (*University of Illinois Chicago*), Hamed Haddadi (*Imperial College London & Brave Software*)

Session 5-3: ML and Security: Generative Models

- **ProFake: Detecting Deepfakes in the Wild against Quality Degradation with Progressive Quality-adaptive Learning** 2207
Huiyu Xu (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*),
Yaopeng Wang (*School of Cyber Science and Engineering, Southeast University*),
Zhibo Wang (*School of Cyber Science and Engineering, Zhejiang University*),
Zhongjie Ba (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*),
Wenxin Liu (*Ant Group*), Lu Jin (*Ant Group*), Haiqin Weng (*Ant Group*), Tao Wei (*Ant Group*),
Kui Ren (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*)
- **Trident of Poseidon: A Generalized Approach for Detecting Deepfake Voices** 2222
Thien-Phuc Doan (*Soongsil University*), Hung Dinh-Xuan (*Soongsil University*),
Taewon Ryu (*Soongsil University*), Inho Kim (*Soongsil University*), Woongjae Lee (*Soongsil University*),
Kihun Hong (*Soongsil University*), Souhwan Jung (*Soongsil University*)
- **On the Detectability of ChatGPT Content: Benchmarking, Methodology, and Evaluation through the Lens of Academic Writing**..... 2236
Zeyan Liu (*EECS/I2S, The University of Kansas*), Zijun Yao (*EECS/I2S, The University of Kansas*),
Fengjun Li (*EECS/I2S, The University of Kansas*), Bo Luo (*EECS/I2S, The University of Kansas*)
- **MGTBench: Benchmarking Machine-Generated Text Detection** 2251
Xinlei He (*The Hong Kong University of Science and Technology (Guangzhou)*),
Xinyue Shen (*CISPA Helmholtz Center for Information Security*),
Zeyuan Chen (*CISPA Helmholtz Center for Information Security*),
Michael Backes (*CISPA Helmholtz Center for Information Security*),
Yang Zhang (*CISPA Helmholtz Center for Information Security*)
- **PromSec: Prompt Optimization for Secure Generation of Functional Source Code with Large Language Models (LLMs)** 2266
Mahmoud Nazzal (*New Jersey Institute of Technology*), Issa Khalil (*Qatar Computing Research Institute*),
Abdallah Khreishah (*New Jersey Institute of Technology*), NhatHai Phan (*New Jersey Institute of Technology*)
- **Dye4AI: Assuring Data Boundary on Generative AI Services**..... 2281
Shu Wang (*George Mason University*), Kun Sun (*George Mason University*), Yan Zhai (*Visa Inc.*)

Session 5-4: Software Security: Embedded Systems and IoT Security

- **Rust for Embedded Systems: Current State and Open Problems** 2296
Ayushi Sharma (*Purdue University*), Shashank Sharma (*Purdue University*),
Sai Ritvik Tanksalkar (*Purdue University*), Santiago Torres-Arias (*Purdue University*),
Aravind Machiry (*Purdue University*)

- **BASEMIRROR: Automatic Reverse Engineering of Baseband Commands from Android's Radio Interface Layer** 2311
Wenqiang Li (*The Ohio State University*), Haohuang Wen (*The Ohio State University*), Zhiqiang Lin (*The Ohio State University*)
- **CANCAL: Towards Real-time and Lightweight Ransomware Detection and Response in Industrial Environments** 2326
Shenao Wang (*Huazhong University of Science and Technology*), Feng Dong (*Huazhong University of Science and Technology*), Hangfeng Yang (*Sangfor Technologies Inc.*), Jingheng Xu (*Sangfor Technologies Inc.*), Haoyu Wang (*Huazhong University of Science and Technology*)
- **RIOTFUZZER: Companion App Assisted Remote Fuzzing for Detecting Vulnerabilities in IoT Devices** 2341
Kaizheng Liu (*Southeast University*), Ming Yang (*Southeast University*), Zhen Ling (*Southeast University*), Yue Zhang (*Drexel University*), Chongqing Lei (*Southeast University*), Junzhou Luo (*Southeast University*), Xinwen Fu (*University of Massachusetts Lowell*)
- **OctopusTaint: Advanced Data Flow Analysis for Detecting Taint-Based Vulnerabilities in IoT/IIoT Firmware** 2355
Abdullah Qasem (*Security Research Centre, Concordia University*), Mourad Debbabi (*Security Research Centre, Concordia University*), Andrei Soeanu (*Security Research Centre, Concordia University*)
- **AutoPatch: Automated Generation of Hotpatches for Real-Time Embedded Devices** 2370
Mohsen Salehi (*The University of British Columbia*), Karthik Pattabiraman (*The University of British Columbia*)

Session 5-5: Applied Crypto: Key management

- **Obfuscated Key Exchange** 2385
Felix Günther (*IBM Research Europe - Zurich*), Douglas Stebila (*University of Waterloo*), Shannon Veitch (*ETH Zurich*)
- **Quarantined-TreeKEM: A Continuous Group Key Agreement for MLS, Secure in Presence of Inactive Users** 2400
Céline Chevalier (*DIENS, École normale supérieure, PSL University, CNRS, INRIA & CRED, Université Panthéon-Assas Paris II*), Guirec Lebrun (*DIENS, École normale supérieure, PSL University, CNRS, INRIA & ANSSI*), Ange Martinelli (*ANSSI*), Abdul Rahman Taleb (*ANSSI*)
- **Complete Knowledge: Preventing Encumbrance of Cryptographic Secrets** 2415
Mahimna Kelkar (*Cornell Tech*), Kushal Babel (*Cornell Tech*), Philip Daian (*Cornell Tech*), James Austgen (*Cornell Tech*), Vitalik Buterin (*Ethereum Foundation*), Ari Juels (*Cornell Tech*)
- **The Insecurity of Masked Comparisons: SCAs on ML-KEM's FO-Transform** 2430
Julius Hermelink (*Max Planck Institute for Security and Privacy*), Kai-Chun Ning (*Max Planck Institute for Security and Privacy*), Richard Petri (*Max Planck Institute for Security and Privacy*), Emanuele Strieder (*Fraunhofer AISEC & Technical University of Munich*)
- **Password-Protected Key Retrieval with(out) HSM Protection** 2445
Sebastian Faller (*IBM Research Europe & ETH Zurich*), Tobias Handirk (*Bergische Universität Wuppertal*), Julia Hesse (*IBM Research Europe*), Máté Horváth (*Bergische Universität Wuppertal*), Anja Lehmann (*Hasso-Plattner-Institute, University of Potsdam*)
- **Non-Transferable Anonymous Tokens by Secret Binding** 2460
F. Betül Durak (*Microsoft Research*), Laurane Marco (*EPFL*), Abdullah Talayhan (*EPFL*), Serge Vaudenay (*EPFL*)

Session 5-6: Applied Crypto: Homomorphic Encryption

- **DPad-HE: Towards Hardware-friendly Homomorphic Evaluation using 4-Directional Manipulation** 2475
Wenxu Tang (*School of Cyber Science and Technology, University of Science and Technology of China*), Fangyu Zheng (*School of Cryptology, University of Chinese Academy of Sciences*), Guang Fan (*School of Cryptology, University of Chinese Academy of Sciences*), Tian Zhou (*School of Cyber Science and Technology, University of Science and Technology of China*), Jingqiang Lin (*School of Cyber Science and Technology, University of Science and Technology of China*), Jiwu Jing (*School of Cryptology, University of Chinese Academy of Sciences*)

- **Rhombus: Fast Homomorphic Matrix-Vector Multiplication for Secure Two-Party Inference** 2490
 Jiaxing He (*Digital Technologies, Ant Group*), Kang Yang (*State Key Laboratory of Cryptology*),
 Guofeng Tang (*Digital Technologies, Ant Group*), Zhangjie Huang (*Digital Technologies, Ant Group*),
 Li Lin (*Digital Technologies, Ant Group*), Changzheng Wei (*Digital Technologies, Ant Group*),
 Ying Yan (*Digital Technologies, Ant Group*), Wei Wang (*Digital Technologies, Ant Group*)
- **Attacks Against the IND-CPA^D Security of Exact FHE Schemes** 2505
 Jung Hee Cheon (*Seoul National University & CryptoLab Inc.*), Hyeongmin Choe (*Seoul National University*),
 Alain Passelègue (*CryptoLab Inc.*), Damien Stehlé (*CryptoLab Inc.*),
 Elias Suvanto (*CryptoLab Inc. & The University of Luxembourg*)
- **VERITAS: Plaintext Encoders for Practical Verifiable Homomorphic Encryption** 2520
 Sylvain Chatel (*CISPA Helmholtz Center for Information Security*), Christian Knabenhans (*SPRING Lab, EPFL*),
 Apostolos Pyrgelis (*RISE Research Institutes of Sweden*), Carmela Troncoso (*SPRING Lab, EPFL*),
 Jean-Pierre Hubaux (*EPFL*)
- **Simpler and Faster BFV Bootstrapping for Arbitrary Plaintext Modulus from CKKS** 2535
 Jaehyung Kim (*CryptoLab Inc.*), Jinyeong Seo (*Seoul National University*),
 Yongsoo Song (*Seoul National University*)
- **New Secret Keys for Enhanced Performance in (T)FHE** 2547
 Loris Bergerat (*Zama & Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC*), Ilaria Chillotti (*Researcher*),
 Damien Ligier (*Researcher*), Jean-Baptiste Orfila (*Zama*),
 Adeline Roux-Langlois (*Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC*), Samuel Tap (*Zama*)

Session 5-7: Blockchain and Distributed Systems: Distributed Ledger Scalability

- **Payout Races and Congested Channels: A Formal Analysis of Security in the Lightning Network** 2562
 Ben Weintraub (*Northeastern University*), Satwik Prabhu Kumble (*TU Delft*),
 Cristina Nita-Rotaru (*Northeastern University*), Stefanie Roos (*University of Kaiserslautern-Landau*)
- **DoubleUp Roll: Double-spending in Arbitrum by Rolling It Back** 2577
 Zhiyuan Sun (*The Hong Kong Polytechnic University & Southern University of Science and Technology*),
 Zihao Li (*The Hong Kong Polytechnic University*), Xinghao Peng (*The Hong Kong Polytechnic University*),
 Xiapu Luo (*The Hong Kong Polytechnic University*), Muhui Jiang (*The Hong Kong Polytechnic University*),
 Hao Zhou (*The Hong Kong Polytechnic University*),
 Yinqian Zhang (*Southern University of Science and Technology*)
- **Rolling in the Shadows: Analyzing the Extraction of MEV Across Layer-2 Rollups** 2591
 Christof Ferreira Torres (*ETH Zurich*), Albin Mamuti (*ETH Zurich*), Ben Weintraub (*Northeastern University*),
 Cristina Nita-Rotaru (*Northeastern University*), Shweta Shinde (*ETH Zurich*)
- **SUI LUTRIS: A Blockchain Combining Broadcast and Consensus** 2606
 Sam Blackshear (*Mysten Labs*), Andrey Chursin (*Mysten Labs*), George Danezis (*Mysten Labs & UCL*),
 Anastasios Kichidis (*Mysten Labs*), Lefteris Kokoris-Kogias (*Mysten Labs & IST Austria*), Xun Li (*Mysten Labs*),
 Mark Logan (*Mysten Labs*), Ashok Menon (*Mysten Labs*), Todd Nowacki (*Mysten Labs*),
 Alberto Sonnino (*Mysten Labs & UCL*), Brandon Williams (*Mysten Labs*), Lu Zhang (*Mysten Labs*)
- **Random Beacons in Monte Carlo: Efficient Asynchronous Random Beacon without Threshold Cryptography** 2621
 Akhil Bandrupalli (*Purdue University*), Adithya Bhat (*Visa Research*), Saurabh Bagchi (*Purdue University*),
 Aniket Kate (*Purdue University / Supra Research*), Michael K. Reiter (*Duke University / Chainlink Labs*)
- **Scalable and Adaptively Secure Any-Trust Distributed Key Generation and All-hands Checkpointing** 2636
 Hanwen Feng (*School of Computer Science, University of Sydney*),
 Tiancheng Mai (*School of Computer Science, University of Sydney*),
 Qiang Tang (*School of Computer Science, University of Sydney*)

Session 6-1: Usability and Measurement: Usable Security

- **Skipping the Security Side Quests: A Qualitative Study on Security Practices and Challenges in Game Development** 2651
Philip Klostermeyer (*CISPA Helmholtz Center for Information Security*), Sabrina Klivan (*CISPA Helmholtz Center for Information Security*), Sandra Höltervennhoff (*Leibniz University Hannover*), Alexander Krause (*CISPA Helmholtz Center for Information Security*), Niklas Busch (*CISPA Helmholtz Center for Information Security*), Sascha Fahl (*CISPA Helmholtz Center for Information Security*)
- **Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises** 2666
Jonas Hielscher (*Chair for Human-Centred Security, Ruhr University Bochum*), Markus Schöps (*Chair for Human-Centred Security, Ruhr University Bochum*), Jens Opdenbusch (*Chair for Human-Centred Security, Ruhr-University Bochum*), Felix Reichmann (*Developer Centered Security, Ruhr University Bochum*), Marco Gutfleisch (*Chair for Human-Centred Security, Ruhr University Bochum*), Karola Marky (*Digital Sovereignty Lab, Ruhr University Bochum*), Simon Parkin (*TPM Cybersecurity Group, Delft University of Technology*)
- **"Modern problems require modern solutions": Community-Developed Techniques for Online Exam Proctoring Evasion** 2681
Lucy Simko (*Barnard College*), Adryana Hutchinson (*The George Washington University*), Alvin Isaac (*The George Washington University*), Evan Fries (*The George Washington University*), Micah Sherr (*Georgetown University*), Adam J. Aviv (*The George Washington University*)
- **"Better Be Computer or I'm Dumb": A Large-Scale Evaluation of Humans as Audio Deepfake Detectors** 2696
Kevin Warren (*University of Florida*), Tyler Tucker (*University of Florida*), Anna Crowder (*University of Florida*), Daniel Olszewski (*University of Florida*), Allison Lu (*University of Florida*), Caroline Fedele (*University of Florida*), Magdalena Pasternak (*University of Florida*), Seth Layton (*University of Florida*), Kevin Butler (*University of Florida*), Carrie Gates (*Dalhousie University*), Patrick Traynor (*University of Florida*)
- **Understanding Legal Professionals' Practices and Expectations in Data Breach Incident Reporting** 2711
Ece Gumusel (*Indiana University Bloomington*), Yue Xiao (*Indiana University Bloomington & IBM Research*), Yue Qin (*Indiana University Bloomington*), Jiaxin Qin (*China University of Political Science and Law*), Xiaojing Liao (*Indiana University Bloomington*)
- **Using AI Assistants in Software Development: A Qualitative Study on Security Practices and Concerns** 2726
Jan H. Klemmer (*CISPA Helmholtz Center for Information Security*), Stefan Albert Horstmann (*Ruhr University Bochum*), Nikhil Patnaik (*University of Bristol*), Cordelia Ludden (*Tufts University*), Cordell Burton Jr. (*Tufts University*), Carson Powers (*Tufts University*), Fabio Massacci (*Vrije Universiteit Amsterdam & University of Trento*), Akond Rahman (*Auburn University*), Daniel Votipka (*Tufts University*), Heather Richter Lipford (*UNC Charlotte*), Awais Rashid (*University of Bristol*), Alena Naiakshina (*Ruhr University Bochum*), Sascha Fahl (*CISPA Helmholtz Center for Information Security*)

Session 6-2: Formal Methods and Programming Languages II

- **SPECMON: Modular Black-Box Runtime Monitoring of Security Protocols** 2741
Kevin Morio (*CISPA Helmholtz Center for Information Security*), Robert Künnemann (*CISPA Helmholtz Center for Information Security*)
- **SemPat: From Hyperproperties to Attack Patterns for Scalable Analysis of Microarchitectural Security** 2756
Adwait Godbole (*University of California, Berkeley*), Yatin A. Manerkar (*University of Michigan*), Sanjit A. Seshia (*University of California, Berkeley*)
- **Block Ciphers in Idealized Models: Automated Proofs and New Security Results** 2771
Miguel Ambrona (*Midnight*), Pooya Farshim (*IOG & Durham University*), Patrick Harasser (*Cryptoplexity, Technische Universität Darmstadt*)

- **Verifiably Correct Lifting of Position-Independent x86-64 Binaries to Symbolized Assembly** 2786
Freek Verbeek (*Open University & Virginia Tech*), Nico Naus (*Open University*), Binoy Ravindran (*Virginia Tech*)
- **Gaussian Elimination of Side-Channels: Linear Algebra for Memory Coloring** 2799
Jana Hofmann (*MPI-SP*), Cédric Fournet (*Azure Research, Microsoft*), Boris Köpf (*Azure Research, Microsoft*), Stavros Volos (*Azure Research, Microsoft*)
- **Foundations for Cryptographic Reductions in CCSA Logics** 2814
David Baelde (*Univ Rennes, CNRS, IRISA*), Adrien Koutsos (*Inria*), Justine Sauvage (*Inria*)

Session 6-3: ML and Security: Federated Learning

- **Distributed Backdoor Attacks on Federated Graph Learning and Certified Defenses** 2829
Yuxin Yang (*College of Computer Science and Technology, Jilin University & Department of Computer Science, Illinois Institute of Technology*),
Qiang Li (*College of Computer Science and Technology, Jilin University*),
Jinyuan Jia (*College of Information Sciences and Technology, The Pennsylvania State University*),
Yuan Hong (*School of Computing, University of Connecticut*),
Binghui Wang (*Department of Computer Science, Illinois Institute of Technology*)
- **Two-Tier Data Packing in RLWE-based Homomorphic Encryption for Secure Federated Learning** 2844
Yufei Zhou (*Guangdong Provincial Key Laboratory of Information Security Technology, School of Computer Science and Engineering, Sun Yat-sen University*),
Peijia Zheng (*Guangdong Provincial Key Laboratory of Information Security Technology, School of Computer Science and Engineering, Sun Yat-sen University*),
Xiaochun Cao (*School of Cyber Science and Technology, Sun Yat-sen University*),
Jiwu Huang (*Guangdong Laboratory of Machine Perception & Intelligent Computing, Faculty of Engineering, Shenzhen MSU-BIT University*)
- **Samplable Anonymous Aggregation for Private Federated Data Analysis**..... 2859
Kunal Talwar (*Apple*), Shan Wang (*Apple*), Audra McMillan (*Apple*), Vitaly Feldman (*Apple*),
Pansy Bansal (*Apple*), Bailey Basile (*Apple*), Aine Cahill (*Apple*), Yi Sheng Chan (*Apple*),
Mike Chatzidakis (*Apple*), Junye Chen (*Apple*), Oliver R. A. Chick (*Apple*), Mona Chitnis (*Apple*),
Suman Ganta (*Apple*), Yusuf Goren (*Apple*), Filip Granqvist (*Apple*), Kristine Guo (*Apple*),
Frederic Jacobs (*Apple*), Omid Javidbakht (*Apple*), Albert Liu (*Apple*), Richard Low (*Apple*),
Dan Mascenik (*Apple*), Steve Myers (*Apple*), David Park (*Apple*), Wonhee Park (*Apple*), Gianni Parsa (*Apple*),
Tommy Pauly (*Apple*), Christian Priebe (*Apple*), Rehan Rishi (*Apple*), Guy N. Rothblum (*Apple*),
Congzheng Song (*Apple*), Linmao Song (*Apple*), Karl Tarbe (*Apple*), Sebastian Vogt (*Apple*),
Shundong Zhou (*Apple*), Vojta Jina (*Researcher*), Michael Scaria (*Base Power Company*),
Luke Winstrom (*Researcher*)
- **Byzantine-Robust Decentralized Federated Learning** 2874
Minghong Fang (*University of Louisville*), Zifan Zhang (*North Carolina State University*),
Hairi (*University of Wisconsin-Whitewater*), Prashant Khanduri (*Wayne State University*),
Jia Liu (*The Ohio State University*), Songtao Lu (*IBM Thomas J. Watson Research Center*),
Yuchen Liu (*North Carolina State University*), Neil Gong (*Duke University*)
- **Not One Less: Exploring Interplay between User Profiles and Items in Untargeted Attacks against Federated Recommendation** 2889
Yurong Hao (*Beijing Jiaotong University*), Xihui Chen (*University of Luxembourg*),
Xiaoting Lyu (*Beijing Jiaotong University*), Jiqiang Liu (*Beijing Jiaotong University*),
Yongsheng Zhu (*Beijing Jiaotong University & China Academy of Railway Sciences Corporation Limited*),
Zhiguo Wan (*Zhejiang Lab*), Sjouke Mauw (*University of Luxembourg*), Wei Wang (*Beijing Jiaotong University*)
- **Unveiling the Vulnerability of Private Fine-Tuning in Split-Based Frameworks for Large Language Models: A Bidirectionally Enhanced Attack**..... 2904
Guanzhong Chen (*Harbin Institute of Technology, Shenzhen*), Zhenghan Qin (*Zhejiang University*),
Mingxin Yang (*Huazhong University of Science and Technology*), Yajie Zhou (*Zhejiang University*),
Tao Fan (*Hong Kong University of Science and Technology & Webank*), Tianyu Du (*Zhejiang University*),
Zenglin Xu (*Fudan University; Shanghai Academy of AI for Science & Pengcheng Lab*)

Session 6-4: Software Security: Access Control and Data Protection

- **PeTAL: Ensuring Access Control Integrity against Data-only Attacks on Linux** 2919
Juhee Kim (*Department of Electrical and Computer Engineering, Seoul National University*),
Jinbum Park (*Samsung Research*),
Yoochan Lee (*Department of Electrical and Computer Engineering, Seoul National University*),
Chengyu Song (*University of California, Riverside*),
Taesoo Kim (*Samsung Research & Georgia Institute of Technology*),
Byoungyoung Lee (*Department of Electrical and Computer Engineering, Seoul National University*)
- **Detecting Broken Object-Level Authorization Vulnerabilities in Database-Backed Applications** 2934
Yongheng Huang (*SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences*),
Chenghang Shi (*SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences*),
Jie Lu (*SKLP, Institute of Computing Technology, CAS*),
Haofeng Li (*SKLP, Institute of Computing Technology, CAS*),
Haining Meng (*SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences*),
Lian Li (*SKLP, Institute of Computing Technology, CAS & University of Chinese Academy of Sciences*)
- **AuthSaber: Automated Safety Verification of OpenID Connect Programs** 2949
Tamjid Al Rahat (*University of California, Los Angeles*), Yu Feng (*University of California, Santa Barbara*),
Yuan Tian (*University of California, Los Angeles*)
- **Unveiling Collusion-Based Ad Attribution Laundering Fraud: Detection, Analysis, and Security Implications** 2963
Tong Zhu (*Shanghai Jiao Tong University*), Chaofan Shou (*University of California, Berkeley*),
Zhen Huang (*Shanghai Jiao Tong University*), Guoxing Chen (*Shanghai Jiao Tong University*),
Xiaokuan Zhang (*George Mason University*), Yan Meng (*Shanghai Jiao Tong University*),
Shuang Hao (*University of Texas at Dallas*), Haojin Zhu (*Shanghai Jiao Tong University*)
- **Gopher: High-Precision and Deep-Dive Detection of Cryptographic API Misuse in the Go Ecosystem** 2978
Yuexi Zhang (*School of Cyber Science and Technology, Beihang University*),
Bingyu Li (*School of Cyber Science and Technology, Beihang University*),
Jingqiang Lin (*School of Cyber Science and Technology, University of Science and Technology of China*),
Linghui Li (*School of Cyberspace Security, Beijing University of Posts and Telecommunications*),
Jiaju Bai (*School of Cyber Science and Technology, Beihang University*),
Shijie Jia (*Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS*),
Qianhong Wu (*School of Cyber Science and Technology, Beihang University*)
- **uMMU: Securing Data Confidentiality with Unobservable Memory Subsystem** 2993
Hajeong Lim (*Sungkyunkwan University*), Jaeyoon Kim (*Sungkyunkwan University*),
Hojoon Lee (*Sungkyunkwan University*)

Session 6-5: Applied Crypto: MPC II

- **Secure Parallel Computation with Oblivious State Transitions** 3008
Nuttapong Attrapadung (*AIST*), Kota Isayama (*SMBC Nikko Securities Inc.*),
Kunihiko Sadakane (*The University of Tokyo*), Kazunari Tozawa (*The University of Tokyo*)
- **Secure Sorting and Selection via Function Secret Sharing** 3023
Amit Agarwal (*University of Illinois Urbana-Champaign*), Elette Boyle (*NTT Research & Reichman University*),
Nishanth Chandran (*Microsoft Research*), Niv Gilboa (*Ben Gurion University*), Divya Gupta (*Microsoft Research*),
Yuval Ishai (*Technion*), Mahimna Kelkar (*Cornell University*), Yiping Ma (*University of Pennsylvania*)
- **Helium: Scalable MPC among Lightweight Participants and under Churn** 3038
Christian Mouchet (*Hasso-Plattner-Institute, University of Potsdam*),
Sylvain Chatel (*CISPA Helmholtz Center for Information Security*),
Apostolos Pyrgelis (*RISE Research Institutes of Sweden*), Carmela Troncoso (*SPRING Lab, EPFL*)
- **Practical Key-Extraction Attacks in Leading MPC Wallets** 3053
Nikolaos Makriyannis (*Fireblocks*), Oren Yomtov (*Fireblocks*), Arik Galansky (*Fireblocks*)
- **Efficient Secret Sharing for Large-Scale Applications** 3065
Sarvar Patel (*Google*), Giuseppe Persiano (*Universita' di Salerno & Google*), Joon Young Seo (*Google*),
Kevin Yeo (*Google & Columbia University*)
- **Oblivious Single Access Machines - A New Model for Oblivious Computation** 3080
Ananya Appan (*University of Illinois at Urbana-Champaign*),
David Heath (*University of Illinois at Urbana-Champaign*), Ling Ren (*University of Illinois at Urbana-Champaign*)

Session 6-6: Applied Crypto: Zero Knowledge Proofs II

- **Tight ZK CPU: Batched ZK Branching with Cost Proportional to Evaluated Instruction** 3095
Yibin Yang (*Georgia Institute of Technology*), David Heath (*University of Illinois Urbana-Champaign*),
Carmit Hazay (*Bar-Ilan University & Ligerio Inc.*),
Vladimir Kolesnikov (*Georgia Institute of Technology*), Muthuramakrishnan Venkatasubramanian (*Ligerio Inc.*)
- **SPARROW: Space-Efficient zkSNARK for Data-Parallel Circuits and Applications to Zero-Knowledge Decision Trees** 3110
Christodoulos Pappas (*Hong Kong University of Science and Technology*),
Dimitrios Papadopoulos (*Hong Kong University of Science and Technology*)
- **The LaZer Library: Lattice-Based Zero Knowledge and Succinct Proofs for Quantum-Safe Privacy** 3125
Vadim Lyubashevsky (*IBM Research Europe*), Gregor Seiler (*IBM Research Europe*),
Patrick Steuer (*IBM Research Europe*)
- **Real-World Universal zkSNARKs are Non-Malleable** 3138
Antonio Faonio (*EURECOM*), Dario Fiore (*IMDEA Software Institute*), Luigi Russo (*EURECOM*)
- **A Succinct Range Proof for Polynomial-based Vector Commitment** 3152
Rui Gao (*Jiangsu Cryptographic Technology Engineering Research Center, Nanjing University of Posts and Telecommunications & Zhejiang Lab*), Zhiguo Wan (*Zhejiang Lab*),
Yuncong Hu (*Department of Computer Science and Engineering, Shanghai Jiao Tong University*),
Huaqun Wang (*Jiangsu Cryptographic Technology Engineering Research Center, Nanjing University of Posts and Telecommunications*)
- **LUNA: Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices** 3167
Ron Steinfeld (*Monash University*), Amin Sakzad (*Monash University*), Muhammed F. Esgin (*Monash University*),
Veronika Kuchta (*Florida Atlantic University*), Mert Yassi (*Monash University*),
Raymond K. Zhao (*CSIRO's Data61*)

Session 6-7: Blockchain and Distributed Systems: Privacy and Consensus

- **zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials** 3182
Foteini Baldimtsi (*Mysten Labs & George Mason University*), Konstantinos Kryptos Chalkias (*Mysten Labs*),
Yan Ji (*Cornell Tech*), Jonas Lindström (*Mysten Labs*), Deepak Maram (*Mysten Labs*),
Ben Riva (*Mysten Labs*), Arnab Roy (*Mysten Labs*), Mahdi Sedaghat (*COSIC, KU Leuven*),
Joy Wang (*Mysten Labs*)
- **Derecho: Privacy Pools with Proof-Carrying Disclosures** 3197
Josh Beal (*Yale University*), Ben Fisch (*Yale University*)
- **Arke: Scalable and Byzantine Fault Tolerant Privacy-Preserving Contact Discovery** 3212
Nicolas Mohnblatt (*Geometry Research*), Alberto Sonnino (*Mysten Labs & University College London*),
Kobi Gurkan (*Geometry Research*), Philipp Jovanovic (*University College London*)
- **Atomic and Fair Data Exchange via Blockchain** 3227
Ertem Nusret Tas (*Stanford University*), István András Seres (*Eötvös Loránd University*),
Yinuo Zhang (*University of California, Berkeley*), Márk Melczer (*Eötvös Loránd University & Guild.xyz*),
Mahimna Kelkar (*Cornell University & Cornell Tech*),
Joseph Bonneau (*A16Z Crypto Research & New York University*), Valeria Nikolaenko (*A16Z Crypto Research*)
- **Asynchronous Consensus without Trusted Setup or Public-Key Cryptography** 3242
Sourav Das (*University of Illinois at Urbana Champaign*), Sisi Duan (*Tsinghua University*),
Shengqi Liu (*Southern University of Science and Technology*),
Atsuki Momose (*University of Illinois at Urbana-Champaign*),
Ling Ren (*University of Illinois at Urbana-Champaign*), Victor Shoup (*Offchain Labs*)
- **Asynchronous Authentication** 3257
Marwa Mouallem (*Technion*), Ittay Eyal (*Technion*)

Session 7-1: Security of Cyber-physical Systems

- **PG: Byzantine Fault-Tolerant and Privacy-Preserving Sensor Fusion with Guaranteed Output Delivery** 3272
Chenglu Jin (*Centrum Wiskunde & Informatica*),
Chao Yin (*Vrije Universiteit Amsterdam & Centrum Wiskunde & Informatica*),
Marten van Dijk (*Centrum Wiskunde & Informatica & Vrije Universiteit Amsterdam*),
Sisi Duan (*Tsinghua University*), Fabio Massacci (*Vrije Universiteit Amsterdam & The University of Trento*),
Michael K. Reiter (*Duke University*),
Haibin Zhang (*Yangtze Delta Region Institute of Tsinghua University, Zhejiang and Beijing Institute of Technology*)
- **A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems** 3287
Lingjing Yu (*Institute of Information Engineering, Chinese Academy of Sciences & Xingditansuo Co., Ltd*),
Jingli Hao (*Xingditansuo Co., Ltd*), Jun Ma (*Sinsegys (Shenzhen) Computer System Co., Ltd.*),
Yong Sun (*Institute of Information Engineering, Chinese Academy of Sciences*),
Yijun Zhao (*Institute of Information Engineering, Chinese Academy of Sciences*),
Bo Luo (*EECS and I2S, The University of Kansas*)
- **GPSBuster: Busting out Hidden GPS Trackers via MSoC Electromagnetic Radiations** 3302
Yue Li (*Hunan University*), Zhenxiong Yan (*Hunan University*), Wenqiang Jin (*Hunan University*),
Zhenyu Ning (*Hunan University*), Daibo Liu (*Hunan University*), Zheng Qin (*Hunan University*),
Yu Liu (*Hunan University*), Huadi Zhu (*Boise State University*), Ming Li (*The University of Texas at Arlington*)
- **Accurate and Efficient Recurring Vulnerability Detection for IoT Firmware** 3317
Haoyu Xiao (*Fudan University*), Yuan Zhang (*Fudan University*), Minghang Shen (*Fudan University*),
Chaoyang Lin (*Fudan University*),
Can Zhang (*State Key Laboratory of Mathematical Engineering and Advanced Computing*),
Shengli Liu (*State Key Laboratory of Mathematical Engineering and Advanced Computing*),
Min Yang (*Fudan University*)

Session 7-2: HW & CPS 5: Attacks in the Physical World

- **RISiren: Wireless Sensing System Attacks via Metasurface** 3332
Chenghan Jiang (*Northwest University*), Jinjiang Yang (*Northwest University*), Xinyi Li (*Tsinghua University*),
Qi Li (*Tsinghua University & Zhongguancun Laboratory*), Xinyu Zhang (*University of California San Diego*),
Ju Ren (*Tsinghua University & Zhongguancun Laboratory*)
- **The Invisible Polyjuice Potion: an Effective Physical Adversarial Attack against Face Recognition** 3346
Ye Wang (*The University of Kansas*), Zeyan Liu (*The University of Kansas*), Bo Luo (*The University of Kansas*),
Rongqing Hui (*The University of Kansas*), Fengjun Li (*The University of Kansas*)
- **RefleXnoop: Passwords Snooping on NLoS Laptops Leveraging Screen-Induced Sound Reflection** 3361
Penghao Wang (*Ocean University of China*), Jingzhi Hu (*Nanyang Technological University*),
Chao Liu (*Ocean University of China*), Jun Luo (*Nanyang Technological University*)
- **UWBAD: Towards Effective and Imperceptible Jamming Attacks Against UWB Ranging Systems with COTS Chips** 3376
Yuqiao Yang (*UESTC*), Zhongjie Wu (*GoGoByte Technology*), Yongzhao Zhang (*UESTC*),
Ting Chen (*UESTC*), Jun Li (*GoGoByte Technology*), Jie Yang (*UESTC*),
Wenhao Liu (*GoGoByte Technology*), Xiaosong Zhang (*UESTC*), Ruicong Shi (*GoGoByte Technology*),
Jingwei Li (*UESTC*), Yu Jiang (*Tsinghua University*), Zhuo Su (*Tsinghua University*)

Session 7-3: HW & CPS: Security of Circuit Design and FPGAs

- **Stealing Maggie's Secrets—On the Challenges of IP Theft Through FPGA Reverse Engineering** 3391
Simon Klix (*Max Planck Institute for Security and Privacy (MPI-SP)*),
Nils Altbartus (*Max Planck Institute for Security and Privacy (MPI-SP)*),
Julian Speith (*Max Planck Institute for Security and Privacy (MPI-SP)*),
Paul Staat (*Max Planck Institute for Security and Privacy (MPI-SP)*),
Alice Verstege (*Max Planck Institute for Security and Privacy (MPI-SP)*),
Annika Wilde (*Ruhr University Bochum*), Daniel Lammers (*Ruhr University Bochum*),
Jörn Langheinrich (*Max Planck Institute for Security and Privacy (MPI-SP)*),
Christian Kison (*Bundeskriminalamt*), Sebastian Sester-Wehle (*Bundeskriminalamt*),
Daniel Holcomb (*UMass Amherst*), Christof Paar (*Max Planck Institute for Security and Privacy (MPI-SP)*)

- **Glitch-Stopping Circuits: Hardware Secure Masking without Registers** 3406
Zhenda Zhang (*COSIC, KU Leuven*), Svetla Petkova-Nikova (*COSIC, KU Leuven*),
Ventzislav Nikov (*NXP Semiconductors*)
- **Whipping the Multivariate-based MAYO Signature Scheme using Hardware Platforms** 3421
Florian Hirner (*Graz University of Technology*), Michael Streibl (*Graz University of Technology*),
Florian Krieger (*Graz University of Technology*), Ahmet Can Mert (*Graz University of Technology*),
Sujoy Sinha Roy (*Graz University of Technology*)
- **CiMSAT: Exploiting SAT Analysis to Attack Compute-in-Memory Architecture Defenses** ... 3436
Jianfeng Wang (*Electronic Engineering, Tsinghua University*),
Huazhong Yang (*Electronic Engineering, Tsinghua University*),
Shuwen Deng (*Electronic Engineering, Tsinghua University*),
Xueqing Li (*Electronic Engineering, Tsinghua University*)

Session 7-4: Privacy and Anonymity: Membership Inference Attacks

- **QueryCheetah: Fast Automated Discovery of Attribute Inference Attacks Against Query-Based Systems** 3451
Bozhidar Stevanoski (*Imperial College London*), Ana-Maria Cretu (*EPFL*),
Yves-Alexandre de Montjoye (*Imperial College London*)
- **Analyzing Inference Privacy Risks Through Gradients In Machine Learning** 3466
Zhuohang Li (*Vanderbilt University*), Andrew Lowy (*University of Wisconsin-Madison*),
Jing Liu (*Mitsubishi Electric Research Laboratories*),
Toshiaki Koike-Akino (*Mitsubishi Electric Research Laboratories*),
Kieran Parsons (*Mitsubishi Electric Research Laboratories*), Bradley Malin (*Vanderbilt University*),
Ye Wang (*Mitsubishi Electric Research Laboratories*)
- **Membership Inference Attacks Against In-Context Learning** 3481
Rui Wen (*CISPA Helmholtz Center for Information Security*),
Zheng Li (*CISPA Helmholtz Center for Information Security*),
Michael Backes (*CISPA Helmholtz Center for Information Security*),
Yang Zhang (*CISPA Helmholtz Center for Information Security*)
- **SeqMIA: Sequential-Metric Based Membership Inference Attack** 3496
Hao Li (*Institute of Software, Chinese Academy of Sciences*),
Zheng Li (*CISPA Helmholtz Center for Information Security*),
Siyuan Wu (*Institute of Software, Chinese Academy of Sciences*),
Chengrui Hu (*Institute of Software, Chinese Academy of Sciences*),
Yutong Ye (*Institute of Software, Chinese Academy of Sciences & Zhongguancun Laboratory*),
Min Zhang (*Institute of Software, Chinese Academy of Sciences*),
Dengguo Feng (*Institute of Software, Chinese Academy of Sciences*),
Yang Zhang (*CISPA Helmholtz Center for Information Security*)

Session 7-5: Privacy and Anonymity: Privacy Attacks Meet ML

- **PreCurious: How Innocent Pre-Trained Language Models Turn into Privacy Traps** 3511
Ruixuan Liu (*Emory University*), Tianhao Wang (*University of Virginia*),
Yang Cao (*Tokyo Institute of Technology*), Li Xiong (*Emory University*)
- **Uncovering Gradient Inversion Risks in Practical Language Model Training** 3525
Xinguo Feng (*The University of Queensland*), Zhongkui Ma (*The University of Queensland*),
Zihan Wang (*The University of Queensland*), Eu Joe Chegne (*The University of Queensland*),
Mengyao Ma (*The University of Queensland*), Alsharif Abuadbba (*CSIRO's Data61*),
Guangdong Bai (*The University of Queensland*)
- **Curator Attack: When Blackbox Differential Privacy Auditing Loses Its Power** 3540
Shiming Wang (*Shanghai Jiao Tong University*), Liyao Xiang (*Shanghai Jiao Tong University*),
Bowe Cheng (*Shanghai Jiao Tong University*), Zhe Ji (*Shanghai Jiao Tong University*),
Tianran Sun (*Shanghai Jiao Tong University*), Xinbing Wang (*Shanghai Jiao Tong University*)
- **Data Poisoning Attacks to Locally Differentially Private Frequent Itemset Mining Protocols** 3555
Wei Tong (*State Key Laboratory for Novel Software Technology, Nanjing University*),
Haoyu Chen (*State Key Laboratory for Novel Software Technology, Nanjing University*),
Jiacheng Niu (*State Key Laboratory for Novel Software Technology, Nanjing University*),
Sheng Zhong (*State Key Laboratory for Novel Software Technology, Nanjing University*)

Session 7-6: Privacy: Defenses and Attacks

- **TabularMark: Watermarking Tabular Datasets for Machine Learning** 3570
Yihao Zheng (*Zhejiang University*), Haocheng Xia (*University of Illinois Urbana-Champaign*),
Junyuan Pang (*Zhejiang University*), Jinfei Liu (*Zhejiang University*), Kui Ren (*Zhejiang University*),
Linyang Chu (*McMaster University*), Yang Cao (*Tokyo Institute of Technology*), Li Xiong (*Emory University*)
- **SafeEar: Content Privacy-Preserving Audio Deepfake Detection** 3585
Xinfeng Li (*Zhejiang University*), Kai Li (*Tsinghua University*), Yifan Zheng (*Zhejiang University*),
Chen Yan (*Zhejiang University*), Xiaoyu Ji (*Zhejiang University*), Wenyuan Xu (*Zhejiang University*)
- **PLEAK: Prompt Leaking Attacks against Large Language Model Applications** 3600
Bo Hui (*Johns Hopkins University*), Haolin Yuan (*Johns Hopkins University*), Neil Gong (*Duke University*),
Philippe Burlina (*Johns Hopkins University Applied Physics Laboratory*), Yinzhi Cao (*Johns Hopkins University*)
- **A Framework for Differential Privacy Against Timing Attacks** 3615
Zachary Ratliff (*Harvard University*), Salil Vadhan (*Harvard University*)

Session 8-1: Network Security: Traffic Analysis and Exploits

- **Exploiting Temporal Vulnerabilities for Unauthorized Access in Intent-based Networking** 3630
Ben Weintraub (*MIT Lincoln Laboratory & Northeastern University*), Jiwon Kim (*Purdue University*),
Ran Tao (*Georgetown University*), Cristina Nita-Rotaru (*Northeastern University*),
Hamed Okhravi (*MIT Lincoln Laboratory*), Dave (Jing) Tian (*Purdue University*),
Benjamin E. Ujcich (*Georgetown University*)
- **PIC-BI: Practical and Intelligent Combinatorial Batch Identification for UAV assisted IoT Networks** 3645
Zhe Ren (*State Key Laboratory of Integrated Services Networks, Xidian University & School of Cyber Engineering, Xidian University*),
Xinghua Li (*State Key Laboratory of Integrated Services Networks, Xidian University & School of Cyber Engineering, Xidian University*),
Yinbin Miao (*State Key Laboratory of Integrated Services Networks, Xidian University & School of Cyber Engineering, Xidian University*),
Mengyao Zhu (*State Key Laboratory of Integrated Services Networks, Xidian University & School of Cyber Engineering, Xidian University*),
Shunjie Yuan (*State Key Laboratory of Integrated Services Networks, Xidian University & School of Cyber Engineering, Xidian University*),
Robert H. Deng (*School of Computing and Information Systems, Singapore Management University*)
- **Detecting Tunneled Flooding Traffic via Deep Semantic Analysis of Packet Length Patterns** 3659
Chuanpu Fu (*Tsinghua University*), Qi Li (*Tsinghua University & Zhongguancun Lab*),
Meng Shen (*Beijing Institute of Technology*), Ke Xu (*Tsinghua University & Zhongguancun Lab*)
- **Release the Hounds! Automated Inference and Empirical Security Evaluation of Field-Deployed PLCs Using Active Network Data** 3674
Ryan Pickren (*Georgia Institute of Technology*), Animesh Chhotaray (*Georgia Institute of Technology*),
Frank Li (*Georgia Institute of Technology*), Saman Zonouz (*Georgia Institute of Technology*),
Raheem Beyah (*Georgia Institute of Technology*)
- **BinPRE: Enhancing Field Inference in Binary Analysis Based Protocol Reverse Engineering** 3689
Jiayi Jiang (*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University*),
Xiyuan Zhang (*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University*),
Chengcheng Wan (*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University*),
Haoyi Chen (*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University*),
Haiying Sun (*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University*),
Ting Su (*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University*)
- **Manipulating OpenFlow Link Discovery Packet Forwarding for Topology Poisoning** 3704
Mingming Chen (*The Pennsylvania State University*), Thomas La Porta (*The Pennsylvania State University*),
Teryl Taylor (*IBM Research*), Frederico Araujo (*IBM Research*), Trent Jaeger (*University of California, Riverside*)

Session 8-2: Software Security: Fuzzing II

- **\$Fuzz to the Future:\$ Uncovering Occluded Future Vulnerabilities via Robust Fuzzing** 3719
Arvind S. Raj (*Arizona State University*), Wil Gibbs (*Arizona State University*),
Fangzhou Dong (*Arizona State University*), Jayakrishna Menon Vadayath (*Arizona State University*),
Michael Tompkins (*Arizona State University*), Steven Wirsz (*Arizona State University*),
Yibo Liu (*Arizona State University*), Zhenghao Hu (*New York University*), Chang Zhu (*Arizona State University*),
Gokulkrishna Praveen Menon (*Arizona State University*), Brendan Dolan-Gavitt (*New York University*),
Adam Doupé (*Arizona State University*), Ruoyu Wang (*Arizona State University*),
Yan Shoshitaishvili (*Arizona State University*), Tiffany Bao (*Arizona State University*)
- **Fuzzing JavaScript Engines with a Graph-based IR** 3734
Haoran Xu (*NUDT*), Zhiyuan Jiang (*NUDT*), Yongjun Wang (*NUDT*), Shuhui Fan (*NUDT*), Shenglin Xu (*NUDT*),
Peidai Xie (*NUDT*), Shaojing Fu (*NUDT*), Mathias Payer (*EPFL*)
- **CrossFire: Fuzzing macOS Cross-XPU Memory on Apple Silicon** 3749
Jiaxun Zhu (*Zhejiang University*), Minghao Lin (*Zhejiang University*), Tingting Yin (*Zhongguancun Laboratory*),
Zechao Cai (*Columbia University*), Yu Wang (*Cyberserval Co., Ltd.*), Rui Chang (*Zhejiang University*),
Wenbo Shen (*Zhejiang University*)
- **Leveraging Binary Coverage for Effective Generation Guidance in Kernel Fuzzing** 3763
Jianzhong Liu (*Tsinghua University*), Yuheng Shen (*Tsinghua University*), Yiru Xu (*Tsinghua University*),
Yu Jiang (*Tsinghua University*)
- **LIFTFUZZ: Validating Binary Lifters through Context-aware Fuzzing with GPT** 3778
Yutong Zhou (*The Chinese University of Hong Kong*), Fan Yang (*The Chinese University of Hong Kong*),
Zirui Song (*The Chinese University of Hong Kong*), Ke Zhang (*The Chinese University of Hong Kong*),
Jiongyi Chen (*National University of Defense Technology*), Kehuan Zhang (*The Chinese University of Hong Kong*)
- **Prompt Fuzzing for Fuzz Driver Generation** 3793
Yunlong Lyu (*Tencent Security Big Data Lab*), Yuxuan Xie (*Tencent Security Big Data Lab*),
Peng Chen (*Tencent Security Big Data Lab*), Hao Chen (*University of California, Davis*)

Session 8-3: ML and Security: Protection Methods in Machine Learning

- **Alchemy: Data-Free Adversarial Training** 3808
Yijie Bai (*Zhejiang University*), Zhongming Ma (*Zhejiang University*), Yanjiao Chen (*Zhejiang University*),
Jiangyi Deng (*Zhejiang University*), Shengyuan Pang (*Zhejiang University*), Yan Liu (*Ant Group*),
Wenyuan Xu (*Zhejiang University*)
- **I Don't Know You, But I Can Catch You: Real-Time Defense against Diverse Adversarial Patches for Object Detectors** 3823
Zijin Lin (*Institute of Information Engineering, Chinese Academy of Sciences & School of Cyber Security, University of Chinese Academy of Sciences*),
Yue Zhao (*Institute of Information Engineering, Chinese Academy of Sciences*),
Kai Chen (*Institute of Information Engineering, Chinese Academy of Sciences & School of Cyber Security, University of Chinese Academy of Sciences*),
Jinwen He (*Institute of Information Engineering, Chinese Academy of Sciences & School of Cyber Security, University of Chinese Academy of Sciences*)
- **Beowulf: Mitigating Model Extraction Attacks Via Reshaping Decision Regions** 3838
Xueluan Gong (*School of Computer Science, Wuhan University*),
Rubin Wei (*School of Cyber Science and Engineering, Wuhan University*),
Ziyao Wang (*School of Cyber Science and Engineering, Wuhan University*),
Yuchen Sun (*School of Cyber Science and Engineering, Wuhan University*),
Jiawen Peng (*School of Cyber Science and Engineering, Wuhan University*),
Yanjiao Chen (*College of Electrical Engineering, Zhejiang University*),
Qian Wang (*School of Cyber Science and Engineering, Wuhan University*)
- **PhySense: Defending Physically Realizable Attacks for Autonomous Systems via Consistency Reasoning** 3853
Zhiyuan Yu (*Washington University in St. Louis*), Ao Li (*Washington University in St. Louis*),
Ruoyao Wen (*Washington University in St. Louis*), Yijia Chen (*Washington University in St. Louis*),
Ning Zhang (*Washington University in St. Louis*)
- **AirGapAgent: Protecting Privacy-Conscious Conversational Agents** 3868
Eugene Bagdasarian (*Google Research*), Ren Yi (*Google Research*), Sahra Ghalebikesabi (*Google Deepmind*),
Peter Kairouz (*Google Research*), Marco Gruteser (*Google Research*), Sewoong Oh (*Google Research*),
Borja Balle (*Google Deepmind*), Daniel Ramage (*Google Research*)

- **ERASER: Machine Unlearning in MLaaS via an Inference Serving-Aware Approach**..... 3883
Yuke Hu (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*),
Jian Lou (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*),
Jiaqi Liu (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*),
Wangze Ni (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University & Hong Kong University of Science and Technology*),
Feng Lin (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*),
Zhan Qin (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*),
Kui Ren (*The State Key Laboratory of Blockchain and Data Security, Zhejiang University*)

Session 8-4: Software Security: Program Analysis and Security Enhancement

- **The HitchHiker's Guide to High-Assurance System Observability Protection with Efficient Permission Switches** 3898
Chuqi Zhang (*School of Computing, National University of Singapore*), Jun Zeng (*Independent Researcher*),
Yiming Zhang (*Southern University of Science and Technology & The Hong Kong Polytechnic University*),
Adil Ahmad (*School of Computing and Augmented Intelligence, Arizona State University*),
Fengwei Zhang (*Department of Computer Science and Engineering, Southern University of Science and Technology*),
Hai Jin (*Huazhong University of Science and Technology*),
Zhenkai Liang (*School of Computing, National University of Singapore*)
- **Eclipse: Preventing Speculative Memory-error Abuse with Artificial Data Dependencies**.... 3913
Neophytos Christou (*Brown University*), Alexander J. Gaidis (*Brown University*),
Vaggelis Atlidakis (*Brown University*), Vasileios P. Kemerlis (*Brown University*)
- **Toss a Fault to BPFChecker: Revealing Implementation Flaws for eBPF runtimes with Differential Fuzzing** 3928
Chaoyuan Peng (*Zhejiang University*), Muhui Jiang (*The Hong Kong Polytechnic University*),
Lei Wu (*Zhejiang University*), Yajin Zhou (*Zhejiang University*)
- **Program Ingredients Abstraction and Instantiation for Synthesis-based JVM Testing** 3943
Yingquan Zhao (*College of Intelligence and Computing, Tianjin University*),
Zan Wang (*College of Intelligence and Computing, Tianjin University*),
Junjie Chen (*College of Intelligence and Computing, Tianjin University*),
Ruifeng Fu (*College of Intelligence and Computing, Tianjin University*),
Yanzhou Lu (*College of Intelligence and Computing, Tianjin University*),
Tianchang Gao (*College of Intelligence and Computing, Tianjin University*),
Haojie Ye (*Programming Language Lab, Huawei*)
- **\$VMud:\$ Detecting Recurring Vulnerabilities with Multiple Fixing Functions via Function Selection and Semantic Equivalent Statement Matching**..... 3958
Kaifeng Huang (*School of Software Engineering, Tongji University*),
Chenhao Lu (*School of Computer Science and Shanghai Key Laboratory of Data Science, Fudan University*),
Yiheng Cao (*School of Computer Science and Shanghai Key Laboratory of Data Science, Fudan University*),
Bihuan Chen (*School of Computer Science and Shanghai Key Laboratory of Data Science, Fudan University*),
Xin Peng (*School of Computer Science and Shanghai Key Laboratory of Data Science, Fudan University*)
- **On Understanding and Forecasting Fuzzers Performance with Static Analysis** 3973
Dongjia Zhang (*EURECOM*), Andrea Fioraldi (*EURECOM*), Davide Balzarotti (*EURECOM*)

Session 8-5: Applied Crypto: Crypto Applied to cloud computing and machine learning

- **End-to-End Encrypted Cloud Storage in the Wild: A Broken Ecosystem** 3988
Jonas Hofmann (*ETH Zurich & Technische Universität Darmstadt*), Kien Tuong Truong (*ETH Zurich*)
- **Scalable Equi-Join Queries over Encrypted Database** 4002
Kai Du (*School of Cyber Engineering, Xidian University*),
Jianfeng Wang (*School of Cyber Engineering, Xidian University*),
Jiaojiao Wu (*School of Cyber Engineering, Xidian University*),
Yunling Wang (*School of Cyberspace Security, Xi'an University of Posts & Telecommunications*)
- **Graphiti: Secure Graph Computation Made More Scalable** 4017
Nishat Koti (*Technical University of Darmstadt*), Varsha Bhat Kukkala (*Independent Researcher*),
Arpita Patra (*Indian Institute of Science*), Bhavish Raj Gopal (*Indian Institute of Science*)

- **CoGNN: Towards Secure and Efficient Collaborative Graph Learning**..... 4032
Zhenhua Zou (*Tsinghua University*), Zhuotao Liu (*Tsinghua University & Zhongguancun Laboratory*),
Jinyong Shan (*Sudo Technology*), Qi Li (*Tsinghua University & Zhongguancun Laboratory*),
Ke Xu (*Tsinghua University & Zhongguancun Laboratory*),
Mingwei Xu (*Tsinghua University & Zhongguancun Laboratory*)
- **PathGES: An Efficient and Secure Graph Encryption Scheme for Shortest Path Queries** 4047
Francesca Falzon (*ETH Zürich*), Esha Ghosh (*Microsoft Research*), Kenneth G. Paterson (*ETH Zürich*),
Roberto Tamassia (*Brown University*)
- **Secure Vickrey Auctions with Rational Parties** 4062
Chaya Ganesh (*Indian Institute of Science*), Shreyas Gupta (*Indian Institute of Science*),
Bhavana Kanukurthi (*Indian Institute of Science*), Girisha Shankar (*Indian Institute of Science*)

Session 8-6: Applied Crypto: ZKPs, Private set operations, Digital Currencies

- **Batching-Efficient RAM using Updatable Lookup Arguments**..... 4077
Moumita Dutta (*Indian Institute of Science*), Chaya Ganesh (*Indian Institute of Science*),
Sikhar Patranabis (*IBM Research India*), Shubh Prakash (*Indian Institute of Science*),
Nitin Singh (*IBM Research India*)
- **Multi-Verifier Zero-Knowledge Proofs for Any Constant Fraction of Corrupted Verifiers**... 4092
Daniel Escudero (*J.P. Morgan AI Research & J.P. Morgan AlgoCRYPT CoE*),
Antigoni Polychroniadou (*J.P. Morgan AI Research & J.P. Morgan AlgoCRYPT CoE*),
Yifan Song (*Tsinghua University & Shanghai Qi Zhi Institute*),
Chenkai Weng (*Arizona State University*)
- **Call Me By My Name: Simple, Practical Private Information Retrieval for Keyword Queries**..... 4107
Sofia Celi (*Brave Software*), Alex Davidson (*Universidade NOVA de Lisboa & NOVA LINC*)
- **Computationally Secure Aggregation and Private Information Retrieval in the Shuffle Model** 4122
Adrià Gascón (*Google*), Yuval Ishai (*Technion*), Mahimna Kelkar (*Cornell University*), Baiyu Li (*Google*),
Yiping Ma (*University of Pennsylvania*), Mariana Raykova (*Google*)
- **Efficient Scalable Multi-Party Private Set Intersection(-Variants) from Bicentric Zero-Sharing** 4137
Ying Gao (*School of Cyber Science and Technology, Beihang University & Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing*),
Yuanhao Luo (*School of Cyber Science and Technology, Beihang University*),
Longxin Wang (*School of Cyber Science and Technology, Beihang University*),
Xiang Liu (*School of Cyber Science and Technology, Beihang University*),
Lin Qi (*School of Cyber Science and Technology, Beihang University*),
Wei Wang (*School of Cyber Science and Technology, Beihang University*),
Mengmeng Zhou (*Beijing Academy of Blockchain and Edge Computing*)
- **High-Throughput Three-Party DPFs with Applications to ORAM and Digital Currencies** ... 4152
Guy Zyskind (*MIT Media Lab*), Avishay Yanai (*Soda Labs*), Alex ‘Sandy’ Pentland (*MIT Media Lab*)

Session 8-7: Usability and Measurement: Phishing, Deepfakes, and Other Risks

- **Employees’ Attitudes towards Phishing Simulations: “It’s like when a child reaches onto the hot hob”**..... 4167
Katharina Schiller (*Hof University of Applied Sciences*), Florian Adamsky (*Hof University of Applied Sciences*),
Christian Eichenmüller (*Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)*),
Matthias Reimert (*Independent Researcher*),
Zinaida Benenson (*Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)*)
- **Content, Nudges and Incentives: A Study on the Effectiveness and Perception of Embedded Phishing Training** 4182
Daniele Lain (*Department of Computer Science, ETH Zurich*),
Tarek Jost (*Department of Computer Science, ETH Zurich*),
Sinisa Matetic (*Department of Computer Science, ETH Zurich*),
Kari Kostianen (*Department of Computer Science, ETH Zurich*),
Srdjan Capkun (*Department of Computer Science, ETH Zurich*)

- **“I Had Sort of a Sense that I Was Always Being Watched...Since I Was”: Examining Interpersonal Discomfort From Continuous Location-Sharing Applications** 4197
Kevin Childs (*University of Florida*), Cassidy Gibson (*University of Florida*), Anna Crowder (*University of Florida*), Kevin Warren (*University of Florida*), Carson Stillman (*University of Florida*), Elissa M. Redmiles (*Georgetown University*), Eakta Jain (*University of Florida*), Patrick Traynor (*University of Florida*), Kevin R. B. Butler (*University of Florida*)
- **When Compiler Optimizations Meet Symbolic Execution: An Empirical Study** 4212
Yue Zhang (*Drexel University*), Melih Sirlanci (*The Ohio State University*), Ruoyu Wang (*Arizona State University*), Zhiqiang Lin (*The Ohio State University*)
- **Defying the Odds: Solana’s Unexpected Resilience in Spite of the Security Challenges Faced by Developers** 4226
Sébastien Andreina (*NEC Laboratories Europe*), Tobias Cloosters (*University of Duisburg-Essen*), Lucas Davi (*University of Duisburg-Essen*), Jens-Rene Giesen (*University of Duisburg-Essen*), Marco Gutfleisch (*Ruhr University Bochum*), Ghassan Karame (*Ruhr University Bochum*), Alena Naiakshina (*Ruhr University Bochum*), Houda Naji (*Ruhr University Bochum*)
- **Unmasking the Security and Usability of Password Masking** 4241
Yuqi Hu (*Georgia Institute of Technology*), Suood Alroomi (*Georgia Institute of Technology & Kuwait University*), Sena Sahin (*Georgia Institute of Technology*), Frank Li (*Georgia Institute of Technology*)

Session 9-1: Applied Crypto: Integrity and Authentication

- **Batch Range Proof: How to Make Threshold ECDSA More Efficient** 4256
Guofeng Tang (*Ant Group*), Shuai Han (*Shanghai Jiao Tong University & Ant Group*), Li Lin (*Ant Group*), Changzheng Wei (*Ant Group*), Ying Yan (*Ant Group*)
- **RSA-Based Dynamic Accumulator without Hashing into Primes** 4271
Victor Youdom Kemmoe (*Brown University*), Anna Lysyanskaya (*Brown University*)
- **Non-interactive VSS using Class Groups and Application to DKG** 4286
Aniket Kate (*Supra Research / Purdue University*), Easwar Vivek Mangipudi (*Supra Research*), Pratyay Mukherjee (*Supra Research*), Hamza Saleem (*University of Southern California / Supra Research*), Sri Aravinda Krishnan Thyagarajan (*University of Sydney*)
- **zkPi: Proving Lean Theorems in Zero-Knowledge** 4301
Evan Laufer (*Stanford University*), Alex Ozdemir (*Stanford University*), Dan Boneh (*Stanford University*)
- **Zero-Knowledge Proofs of Training for Deep Neural Networks** 4316
Kasra Abbaszadeh (*University of Maryland*), Christodoulos Pappas (*Hong Kong University of Science and Technology*), Jonathan Katz (*Google & University of Maryland*), Dimitrios Papadopoulos (*Hong Kong University of Science and Technology*)
- **Multi-User Security of CCM Authenticated Encryption Mode** 4331
Xiangyang Zhang (*Shanghai Jiao Tong University*), Yaobin Shen (*Xiamen University*), Lei Wang (*Shanghai Jiao Tong University*)

Session 9-2: ML and Security: Model Security

- **HYPERTHEFT: Thieving Model Weights from TEE-Shielded Neural Networks via Ciphertext Side Channels** 4346
Yuanyuan Yuan (*The Hong Kong University of Science and Technology*), Zhibo Liu (*The Hong Kong University of Science and Technology*), Sen Deng (*The Hong Kong University of Science and Technology*), Yanzuo Chen (*The Hong Kong University of Science and Technology*), Shuai Wang (*The Hong Kong University of Science and Technology*), Yinqian Zhang (*Southern University of Science and Technology*), Zhendong Su (*ETH Zurich*)
- **NeuJeans: Private Neural Network Inference with Joint Optimization of Convolution and FHE Bootstrapping** 4361
Jae Hyung Ju (*Seoul National University*), Jaiyoung Park (*Seoul National University*), Jongmin Kim (*Seoul National University*), Minsik Kang (*Seoul National University*), Donghwan Kim (*Seoul National University*), Jung Hee Cheon (*Seoul National University & CryptoLab Inc.*), Jung Ho Ahn (*Seoul National University*)

- **Ents: An Efficient Three-party Training Framework for Decision Trees by Communication Optimization** 4376
Guopeng Lin (*Fudan University*), Weili Han (*Fudan University*), Wenqiang Ruan (*Fudan University*), Ruisheng Zhou (*Fudan University*), Lushan Song (*Fudan University*), Bingshuai Li (*Huawei Technologies*), Yunfeng Shao (*Huawei Technologies*)
- **Fast and Accurate Homomorphic Softmax Evaluation**..... 4391
Wonhee Cho (*Department of Mathematics, Seoul National University*), Guillaume Hanrot (*CryptoLab, Inc.*), Taeseong Kim (*Department of Mathematics, Seoul National University*), Minje Park (*CryptoLab, Inc.*), Damien Stehlé (*CryptoLab, Inc.*)
- **zkLLM: Zero Knowledge Proofs for Large Language Models** 4405
Haochen Sun (*University of Waterloo*), Jason Li (*University of Waterloo*), Hongyang Zhang (*University of Waterloo*)
- **AITIA: Efficient Secure Computation of Bivariate Causal Discovery**..... 4420
Truong Son Nguyen (*Arizona State University*), Lun Wang (*UC Berkeley*), Evgenios M. Kornaropoulos (*George Mason University*), Ni Trieu (*Arizona State University*)

Session 9-3: ML and Security: Backdoors, Side Channel Attacks, and Anomaly Detection in Machine Learning

- **Fisher Information guided Purification against Backdoor Attacks**..... 4435
Nazmul Karim (*University of Central Florida*), Abdullah Al Arafat (*North Carolina State University*), Adnan Siraj Rakin (*Binghamton University (SUNY)*), Zhishan Guo (*North Carolina State University*), Nazanin Rahnavard (*University of Central Florida*)
- **BadMerging: Backdoor Attacks Against Model Merging** 4450
Jinghui Zhang (*University of California, Los Angeles*), Jianfeng Chi (*Meta*), Zheng Li (*CISPA Helmholtz Center for Information Security*), Kunlin Cai (*University of California, Los Angeles*), Yang Zhang (*CISPA Helmholtz Center for Information Security*), Yuan Tian (*University of California, Los Angeles*)
- **Watch Out! Simple Horizontal Class Backdoor Can Trivially Evade Defense** 4465
Hua Ma (*CSIRO's Data61*), Shang Wang (*University of Technology Sydney*), Yansong Gao (*CSIRO's Data61*), Zhi Zhang (*The University of Western Australia*), Huming Qiu (*Fudan University*), Minhui Xue (*CSIRO's Data61*), Alsharif Abuadba (*CSIRO's Data61*), Anmin Fu (*Nanjing University of Science and Technology*), Surya Nepal (*CSIRO's Data61*), Derek Abbott (*The University of Adelaide*)
- **Mithridates: Auditing and Boosting Backdoor Resistance of Machine Learning Pipelines**... 4480
Eugene Bagdasarian (*University of Massachusetts Amherst*), Vitaly Shmatikov (*Cornell Tech*)
- **DeepCache: Revisiting Cache Side-Channel Attacks in Deep Neural Networks Executables** 4495
Zhibo Liu (*The Hong Kong University of Science and Technology*), Yuan Yuan (*The Hong Kong University of Science and Technology*), Yanzuo Chen (*The Hong Kong University of Science and Technology*), Sihang Hu (*Huawei Technologies*), Tianxiang Li (*Huawei Technologies*), Shuai Wang (*The Hong Kong University of Science and Technology*)
- **Rules Refine the Riddle: Global Explanation for Deep Learning-Based Anomaly Detection in Security Applications**..... 4509
Dongqi Han (*Tsinghua University & Zhongguancun Laboratory*), Zhiliang Wang (*Tsinghua University & Zhongguancun Laboratory*), Ruitao Feng (*Singapore Management University*), Minghui Jin (*State Grid Shanghai Municipal Electric Power Company*), Wenqi Chen (*Tsinghua University & Zhongguancun Laboratory*), Kai Wang (*Tsinghua University & Zhongguancun Laboratory*), Su Wang (*Zhongguancun Laboratory*), Jiahai Yang (*Tsinghua University & Zhongguancun Laboratory*), Xingang Shi (*Tsinghua University & Zhongguancun Laboratory*), Xia Yin (*Tsinghua University & Zhongguancun Laboratory*), Yang Liu (*Nanyang Technological University*)

Session 9-4: Software Security: Attacks and Defenses

- **Boosting Practical Control-Flow Integrity with Complete Field Sensitivity and Origin Awareness** 4524
Hao Xiang (*School of Cyber Engineering, State Key Lab of ISN, Xidian University*), Zehui Cheng (*School of Cyber Engineering, State Key Lab of ISN, Xidian University*), Jinku Li (*School of Cyber Engineering, State Key Lab of ISN, Xidian University*), Jianfeng Ma (*School of Cyber Engineering, State Key Lab of ISN, Xidian University*), Kangjie Lu (*University of Minnesota-Twins Cities*)

- **PowerPeeler: A Precise and General Dynamic Deobfuscation Method for PowerShell Scripts** 4539
Ruijie Li (*Southeast University & QI-ANXIN Technology Research Institute*),
Chenyang Zhang (*Fudan University*), Huajun Chai (*QI-ANXIN Technology Research Institute*),
Lingyun Ying (*QI-ANXIN Technology Research Institute & Tsinghua University-QI-ANXIN Group JCNS*),
Haixin Duan (*Tsinghua University & Tsinghua University-QI-ANXIN Group JCNS*),
Jun Tao (*Southeast University*)
- **ReSym: Harnessing LLMs to Recover Variable and Data Structure Symbols from Stripped Binaries** 4554
Danning Xie (*Purdue University*), Zhuo Zhang (*Purdue University*), Nan Jiang (*Purdue University*),
Xiangzhe Xu (*Purdue University*), Lin Tan (*Purdue University*), Xiangyu Zhang (*Purdue University*)
- **Manipulative Interference Attacks** 4569
Samuel Mergendahl (*University of Oregon*), Stephen Fickas (*University of Oregon*),
Boyana Norris (*University of Oregon*), Richard Skowrya (*MIT Lincoln Laboratory*)
- **Isolate and Detect the Untrusted Driver with a Virtual Box** 4584
YongGang Li (*School of Computer Science and Technology, China University of Mining and Technology & Mine Digitization Engineering Research Center of the Ministry of Education*),
ShunRong Jiang (*School of Computer Science and Technology, China University of Mining and Technology & Mine Digitization Engineering Research Center of the Ministry of Education*),
Yu Bao (*School of Computer Science and Technology, China University of Mining and Technology & Mine Digitization Engineering Research Center of the Ministry of Education*),
PengPeng Chen (*The China University of Mining School of Computer Science and Technology, China University of Mining and Technology & Mine Digitization Engineering Research Center of the Ministry of Education*),
Yong Zhou (*School of Computer Science and Technology, China University of Mining and Technology & Mine Digitization Engineering Research Center of the Ministry of Education*),
Yeh-Ching Chung (*Chinese University of Hong Kong, Shenzhen*)
- **\$Gramine-TDX: A Lightweight OS Kernel for Confidential VMs** 4598
Dmitrii Kuvaitskii (*Intel Labs*),
Dimitrios Stavrakakis (*The University of Edinburgh & Technical University of Munich*),
Kailun Qin (*Intel Corporation & Shanghai Jiao Tong University*), Cedric Xing (*Intel Corporation*),
Pramod Bhatotia (*Technical University of Munich*), Mona Vij (*Intel Labs*)

Session 9-5: Applied Crypto: Advanced Encryption schemes and their applications

- **ArcEDB: An Arbitrary-Precision Encrypted Database via (Amortized) Modular Homomorphic Encryption** 4613
Zhou Zhang (*Beihang University*), Song Bian (*Beihang University*), Zian Zhao (*Beihang University*),
Ran Mao (*Beihang University*), Haoyi Zhou (*Beihang University & Zhongguancun Laboratory*),
Jiafeng Hua (*Xidian University*), Yier Jin (*University of Science and Technology of China*),
Zhenyu Guan (*Beihang University*)
- **ISABELLA: Improving Structures of Attribute-Based Encryption Leveraging Linear Algebra** . 4628
Doreen Riepel (*UC San Diego*), Marloes Venema (*University of Wuppertal*), Tanya Verma (*Tinfoil*)
- **Conditional Encryption with Applications to Secure Personalized Password Typo Correction** 4643
Mohammad Hassan Ameri (*Purdue University*), Jeremiah Blocki (*Purdue University*)
- **Practical Non-interactive Encrypted Conjunctive Search with Leakage Suppression** 4658
Yunling Wang (*School of Cyberspace Security, Xi'an University of Posts & Telecommunications*),
Shi-Feng Sun (*Shanghai Jiao Tong University & Blockchain Advanced Research Center*),
Jianfeng Wang (*School of Cyber Engineering, Xidian University*),
Xiaofeng Chen (*School of Cyber Engineering, Xidian University*),
Joseph K. Liu (*Faculty of Information Technology, Monash University*),
Dawu Gu (*Shanghai Jiao Tong University & Blockchain Advanced Research Center*)
- **Securely Training Decision Trees Efficiently** 4673
Divyanshu Bhardwaj (*Microsoft Research*), Sandhya Saravanan (*Microsoft Research*),
Nishanth Chandran (*Microsoft Research*), Divya Gupta (*Microsoft Research*)
- **FABESA: Fast (and Anonymous) Attribute-Based Encryption under Standard Assumption** . 4688
Long Meng (*University of Surrey*), Liqun Chen (*University of Surrey*),
Yangguang Tian (*University of Surrey*), Mark Manulis (*Universität der Bundeswehr München*)

Session 9-6: Applied Crypto: Customized cryptographic solutions

- **Pulsar: Secure Steganography for Diffusion Models** 4703
Tushar M. Jois (*City College of New York*), Gabrielle Beck (*Johns Hopkins University*),
Gabriel Kaptchuk (*University of Maryland, College Park*)
- **Protoss: Protocol for Tight Optimal Symmetric Security** 4718
Emanuele Di Giandomenico (*Eindhoven University of Technology*),
Yong Li (*Huawei Technologies Duesseldorf*), Sven Schäge (*Eindhoven University of Technology*)
- **What Did Come Out of It? Analysis and Improvements of DIDComm Messaging** 4732
Christian Badertscher (*IOG & School of Engineering, Zurich University of Applied Sciences*),
Fabio Banfi (*Zühlke Engineering AG*), Jesus Diaz (*IOG*)
- **On the Tight Security of the Double Ratchet**..... 4747
Daniel Collins (*Purdue University & Georgia Tech*), Doreen Riepel (*UC San Diego*),
Si An Oliver Tran (*ETH Zurich*)
- **Fake It till You Make It: Enhancing Security of Bluetooth Secure Connections via
Deferrable Authentication** 4762
Marc Fischlin (*Cryptoplexity, Technische Universität Darmstadt*),
Olga Sanina (*Cryptoplexity, Technische Universität Darmstadt*)
- **Reconstructing with Even Less: Amplifying Leakage and Drawing Graphs** 4777
Evangelia Anna Markatou (*TU Delft & Brown University*), Roberto Tamassia (*Brown University*)

Session 9-7: Usability and Measurement: AI Risks

- **Avara: A Uniform Evaluation System for Perceptibility Analysis Against Adversarial
Object Evasion Attacks** 4792
Xinyao Ma (*Indiana University Bloomington*), Chaoqi Zhang (*Indiana University Bloomington*),
Huadi Zhu (*The University of Texas at Arlington*), L. Jean Camp (*Indiana University Bloomington*),
Ming Li (*The University of Texas at Arlington*), Xiaojing Liao (*Indiana University Bloomington*)
- **SAFEgen: Mitigating Sexually Explicit Content Generation in Text-to-Image Models**..... 4807
Xinfeng Li (*Zhejiang University*), Yuchen Yang (*Johns Hopkins University*),
Jiangyi Deng (*Zhejiang University*), Chen Yan (*Zhejiang University*), Yanjiao Chen (*Zhejiang University*),
Xiaoyu Ji (*Zhejiang University*), Wenyuan Xu (*Zhejiang University*)
- **Organic or Diffused: Can We Distinguish Human Art from AI-generated Images?** 4822
Anna Yoo Jeong Ha (*University of Chicago*), Josephine Passananti (*University of Chicago*),
Ronik Bhaskar (*University of Chicago*), Shawn Shan (*University of Chicago*),
Reid Southen (*Concept Artist*), Haitao Zheng (*University of Chicago*), Ben Y. Zhao (*University of Chicago*)
- **Image-Perfect Imperfections: Safety, Bias, and Authenticity in the Shadow
of Text-To-Image Model Evolution** 4837
Yixin Wu (*CISPA Helmholtz Center for Information Security*), Yun Shen (*Netapp*),
Michael Backes (*CISPA Helmholtz Center for Information Security*),
Yang Zhang (*CISPA Helmholtz Center for Information Security*)
- **ZeroFake: Zero-Shot Detection of Fake Images Generated and Edited
by Text-to-Image Generation Models**..... 4852
Zeyang Sha (*CISPA Helmholtz Center for Information Security*),
Yicong Tan (*CISPA Helmholtz Center for Information Security*),
Mingjie Li (*CISPA Helmholtz Center for Information Security*),
Michael Backes (*CISPA Helmholtz Center for Information Security*),
Yang Zhang (*CISPA Helmholtz Center for Information Security*)
- **Blind and Low-Vision Individuals' Detection of Audio Deepfakes**..... 4867
Filipo Sharevski (*DePaul University*), Aziz Zeidieh (*University of Illinois Urbana-Champaign*),
Jennifer Vander Loop (*DePaul University*), Peter Jachim (*DePaul University*)

Workshop Session I

- **HealthSec '24: First ACM CCS Workshop on Cybersecurity in Healthcare** 4882
William Yurcik (*Centers for Medicare & Medicaid Services (CMS)*),
Gregory Pluta (*University of Illinois at Urbana-Champaign*),
Toan Luong (*MITRE*), Luis Garcia (*University of Utah*)
- **AACD '24: 11th ACM Workshop on Adaptive and Autonomous Cyber Defense** 4884
Neil Gong (*Duke University*), Qi Li (*Tsinghua University*), X
iaoli Zhang (*University of Science and Technology Beijing*)
- **SaTS '24: The 2nd ACM Workshop on Secure and Trustworthy Superapps** 4886
Zhiqiang Lin (*The Ohio State University*), Luyi Xing (*Indiana University Bloomington*)
- **LAMPS '24: ACM CCS Workshop on Large AI Systems and Models with Privacy and Safety Analysis**..... 4888
Bo Li (*University of Chicago*), Wenyan Xu (*Zhejiang University*), Jieshan Chen (*CSIRO's Data61*),
Yang Zhang (*CISPA Helmholtz Center for Information Security*), Minhui Xue (*CSIRO's Data61*),
Shuo Wang (*Shanghai Jiao Tong University*), Guangdong Bai (*University of Queensland*),
Xingliang Yuan (*University of Melbourne*)
- **WAHC'24 – 12th Workshop on Encrypted Computing & Applied Homomorphic Cryptography** 4890
Flavio Bergamaschi (*Intel Corporation*), Anamaria Costache (*Norwegian University of Science and Technology*),
Kurt Rohloff (*Duality Technologies and NJIT*)
- **WPES '24: 23rd Workshop on Privacy in the Electronic Society (WPES)** 4893
Erman Ayday (*Case Western Reserve University*), Jaideep Vaidya (*Rutgers University*)
- **RICSS '24: 2nd International Workshop on Re-design Industrial Control Systems with Security** 4894
Ruimin Sun (*Florida International University*), Mu Zhang (*University of Utah*)
- **The 19th Workshop on Programming Languages and Analysis for Security (PLAS 2024)** 4896
Lesly-Ann Daniel (*DistriNet, KU Leuven*), Vineet Rajani (*University of Kent*)

Workshop Session II

- **FEAST'24: Sixth Workshop on Forming an Ecosystem Around Software Transformation** 4898
Ryan Craven (*Office of Naval Research*), Matthew Mickelson (*MITRE*)
- **CCSW 2024 -- Cloud Computing Security Workshop**..... 4900
Apostolos Fournaris (*Industrial Systems Institute/Research Center ATHENA*),
Paolo Palmieri (*Computer Science, University College Cork*)
- **CheckMATE '24 - Research on Offensive and Defensive Techniques in the context of Man At The End (MATE) Attacks** 4901
Sebastian Schrittwieser (*Christian Doppler Laboratory for Assurance and Transparency in Software Protection, University of Vienna*),
Michele Ianni (*Department of Computer Engineering, Modeling, Electronics and Systems, University of Calabria*)
- **CPSIoTSec'24: The Sixth Workshop on CPS&IoT Security and Privacy** 4903
Kassem Fawaz (*University of Wisconsin-Madison*), Magnus Almgren (*Chalmers University of Technology*)
- **AISeC '24: 17th ACM Workshop on Artificial Intelligence and Security**..... 4905
Maura Pintor (*University of Cagliari*), Matthew Jagielski (*Google DeepMind*),
Xinyun Chen (*Google Deepmind*)
- **DeFi '24: Workshop on Decentralized Finance and Security** 4907
Liyi Zhou (*The University of Sydney*), Kaihua Qin (*Yale University*)
- **ASHES '24 – Workshop on Attacks and Solutions in Hardware Security** 4909
Lejla Batina (*Radboud University*),
Chip Hong Chang (*School of Electrical and Electronic Engineering, Nanyang Technological University*),
Ulrich Rührmair (*TU Berlin and U Connecticut*), Jakub Szefer (*Yale University*)
- **AutonomousCyber'24: Workshop on Autonomous Cybersecurity** 4911
Ali Dehghantanha (*University of Guelph*), Reza M. Parizi (*Kennesaw State University*),
Gregory Epiphaniou (*University of Warwick*)

- **CSCS '24 – Cyber Security in CarS Workshop**..... 4914
Mario Fritz (*CISPA Helmholtz Center for Information Security*),
Christoph Krauß (*Darmstadt University of Applied Sciences*),
Hans-Joachim Hof (*CARISSMA Institute of Electric, Connected, and Secure Mobility, Technische Hochschule Ingolstadt*)
- **SCORED '24: Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses** 4917
Santiago Torres-Arias (*Purdue University*), Marcela Melara (*Intel Corporation*)

Poster Session

- **Poster: Privacy Norms for Fertility Data in the Roe v. Wade era** 4919
Zander Chown (*Skidmore College*), Aarathi Prasad (*Skidmore College*)
- **Poster: Kill Krill or Proxy RPKI** 4922
Louis Cattepoel (*TU Darmstadt*), Donika Mirdita (*TU Darmstadt & ATHENE*),
Haya Schulmann (*Goethe-Univ. Frankfurt & ATHENE*), Michael Waidner (*TU Darmstadt & ATHENE*)
- **Poster: Security of Login Interfaces in Modern Organizations** 4925
Kevin Nsieyanji Tchokodeu (*ATHENE & Technical University Darmstadt*),
Haya Schulmann (*ATHENE & Goethe-University Frankfurt*), Gil Sobol (*ATHENE & Goethe-University Frankfurt*),
Michael Waidner (*ATHENE, Technical University Darmstadt & Fraunhofer SIT*)
- **Poster: Whether We Are Good Enough to Detect Server-Side Request Forgeries in PHP-native Applications?** 4928
Yuchen Ji (*ShanghaiTech University*), Ting Dai (*IBM Research*), Yutian Tang (*University of Glasgow*),
Jingzhu He (*ShanghaiTech University*)
- **Poster: Marian: An Open Source RISC-V Processor with Zvk Vector Cryptography Extensions** 4931
Thomas Szymkowiak (*Tampere University*), Endrit Isufi (*Tampere University*),
Markku-Juhani Saarinen (*Tampere University*)
- **Poster: Towards Real-Time Intrusion Detection with Explainable AI-Based Detector** 4934
Wenhao Li (*Research Institute of China Telecom Corporation Ltd.*),
Duohe Ma (*Institute of Information Engineering, CAS*),
Zhaoxuan Li (*Institute of Information Engineering, Chinese Academy of Science*),
Huafeng Bao (*Tencent Technology (Shenzhen) Co. Ltd.*),
Shuai Wang (*Research Institute of China Telecom Corporation Ltd.*),
Huamin Jin (*Research Institute of China Telecom Corporation Ltd.*),
Xiao-Yu Zhang (*Institute of Information Engineering, Chinese Academy of Science*)
- **Poster: Patching NSEC3-Encloser: The Good, the Bad, and the Ugly** 4937
Oliver Jacobsen (*ATHENE & Goethe-Universität Frankfurt*),
Haya Schulmann (*ATHENE & Goethe-Universität Frankfurt*)
- **Poster: An Exploration of Large Language Models in Malicious Source Code Detection** 4940
Di Xue (*Huawei Technologies Co., Ltd.*), Gang Zhao (*Huawei Technologies Co., Ltd.*),
Zhongqi Fan (*Huawei Technologies Co., Ltd.*), Wei Li (*Huawei Technologies Co., Ltd.*),
Yahong Xu (*Huawei Technologies Co., Ltd.*), Zhen Liu (*Huawei Technologies Co., Ltd.*),
Yin Liu (*Huawei Technologies Co., Ltd.*), Zhongliang Yuan (*Huawei Technologies Co., Ltd.*)
- **Poster: The Concept of a System for Automatic Detection and Correction of Vulnerabilities in the Source Code** 4943
Tomasz Hyla (*West Pomeranian University of Technology in Szczecin*), Natalia Wawrzyniak (*Maritime University of Szczecin*)
- **Poster: Cyber Security Economics Model (CYSEM)** 4946
Tong Xin (*School of Electronic Engineering and Computer Science, Queen Mary University of London*),
Ying He (*School of Electronic Engineering and Computer Science, Queen Mary University of London*),
Efpraxia D. Zamani (*Business School, Durham University Business School*),
Cunjin Luo (*School of Computer Science and Electronic Engineering, University of Essex*)
- **Poster: AuditVotes: A Framework towards Deployable Certified Robustness for GNNs** 4949
Yuni Lai (*The Hong Kong Polytechnic University*), Kai Zhou (*The Hong Kong Polytechnic University*)

- **Poster: zkTax: A Pragmatic Way to Support Zero-Knowledge Tax Disclosures** 4952
Alex Berke (*MIT*), Tobin South (*MIT*), Robert Mahari (*MIT*), Kent Larson (*MIT*),
Alex Pentland (*MIT*)
- **Poster: End-to-End Privacy-Preserving Vertical Federated Learning using Private Cross-Organizational Data Collaboration** 4955
Keiichi Ochiai (*NTT DOCOMO, INC.*), Masayuki Terada (*NTT DOCOMO, INC.*)
- **Poster: YFuzz: Data-Driven Fuzzing**..... 4958
Yuan Chang (*National Taiwan University*), Chun-Chia Huang (*National Taiwan University*),
Tatsuya Mori (*Waseda University*), Hsu-Chun Hsiao (*National Taiwan University & Academia Sinica*)
- **Poster: Repairing Bugs with the Introduction of New Variables: A Multi-Agent Large Language Model** 4961
Elisa Zhang (*Dougherty Valley High School*), Shiyu Sun (*George Mason University*),
Yunlong Xing (*George Mason University*), Kun Sun (*George Mason University*)
- **Poster: In-switch Defense against DNS Amplification DDoS Attacks**..... 4964
Seyed Mohammad Hadi Mirsadeghi (*Tallinn University of Technology*)
- **Poster: A Full-stack Secure Deletion Framework for Modern Computing Devices** 4967
Bo Chen (*Department of Computer Science, Michigan Technological University*),
Caleb Rother (*Department of Computer Science, Michigan Technological University*),
Josh Dafoe (*Department of Computer Science, Michigan Technological University*)
- **Poster: Few-Shot Inter-Domain Routing Threat Detection with Large-Scale Multi-Modal Pre-Training** 4970
Yizhi Li (*INSC, Tsinghua University*), Jiang Li (*Zhongguancun Laboratory*),
Jiahao Cao (*INSC, Tsinghua University*), Renjie Xie (*INSC, Tsinghua University*),
Yangyang Wang (*INSC, Tsinghua University*), Mingwei Xu (*INSC, Tsinghua University*)
- **Poster: Formally Verified Binary Lifting to P-Code** 4973
Nico Naus (*Open University & Virginia Tech*), Freek Verbeek (*Open University & Virginia Tech*),
Sagar Atla (*Virginia Tech*), Binoy Ravindran (*Virginia Tech*)
- **Poster: libdebug, Build Your Own Debugger for a Better (Hello) World**..... 4976
Gabriele Digregorio (*Politecnico di Milano*), Roberto Alessandro Bertolini (*Politecnico di Milano*),
Francesco Panebianco (*Politecnico di Milano*), Mario Polino (*Unaffiliated*)
- **Poster: \$M^2ASK: A Correlation-Based Multi-Step Attack Scenario Detection Framework Using MITRE ATT&CK Mapping** 4979
Qiaoran Meng (*National University of Singapore*), Nay Oo (*NCS Cyber Special Ops-R&D*),
Yuning Jiang (*National University of Singapore*), Hoon Wei Lim (*NCS Cyber Special Ops-R&D*),
Biplab Sikdar (*National University of Singapore*)
- **Poster: Synchronization Concerns of DNS Integrations** 4982
Andrew Kaizer (*Verisign*), Will Naciri (*Verisign*), Swapneel Sheth (*Verisign*)
- **Poster: E-Graphs and Equality Saturation for Term-Rewriting in MBA Deobfuscation: An Empirical Study** 4985
Seoksu Lee (*Chungnam National University*), Hyeonchang Jeon (*Chungnam National University*),
Eun-Sun Cho (*Chungnam National University*)
- **Poster: Different Victims, Same Layout: Email Visual Similarity Detection for Enhanced Email Protection** 4988
Sachin Shukla (*Cisco Talos*), Omid Mirzaei (*Cisco Talos*)
- **Poster: Formalizing Cognitive Biases for Cybersecurity Defenses** 4991
Jasmine Vang (*Montana State University*), Matthew Revelle (*Montana State University*)
- **Poster: TAPChecker: Model Checking in Trigger-Action Rules Generation Using Large Language Models** 4994
Huan Bui (*Department of Software Information Systems, The University of North Carolina at Charlotte*),
Harper Lienerth (*Department of Mathematics and Computer Science, Albion College*),
Chenglong Fu (*Department of Software Information Systems, The University of North Carolina at Charlotte*),
Meera Sridhar (*Department of Software Information Systems, The University of North Carolina at Charlotte*)
- **Poster: Gift or Curse? Safety Slider Settings in Tor Website Fingerprinting**..... 4997
Joel Osher (*University of Minnesota*), James K. Holland (*University of Minnesota*),
Nicholas Hopper (*University of Minnesota*)

- **Poster: Detecting Ransomware Attacks by Analyzing Replicated Block Snapshots Using Neural Networks** 5000
Seok Min Hong (*Hanyang University ERICA*), Beom Heyn Kim (*Hanyang University ERICA*),
Mohammad Mannan (*Concordia University*)
- **Poster: Multiparty Private Set Intersection from Multiparty Homomorphic Encryption** 5003
Christian Mouchet (*Hasso-Plattner-Institute, University of Potsdam*),
Sylvain Chatel (*CISPA Helmholtz Center for Information Security*), Lea Nürnberger (*NTNU*),
Wouter Lueks (*CISPA Helmholtz Center for Information Security*)
- **Poster: Post-Quantum Identity-Based Matching Encryption with Revocable Decryption Key**..... 5006
Jheng-Jia Huang (*Dept of Information Management, National Taiwan University of Science and Technology*),
Guan-Yu Chen (*Dept of Information Management, National Taiwan University of Science and Technology*),
Nai-Wei Lo (*Dept of Information Management, National Taiwan University of Science and Technology*)
- **Poster: A Multi-step Approach for Classification of Malware Samples** 5009
Arnaldo Sgueglia (*University of Sannio*), Rocco Addabbo (*TIM*), Andrea Di Sorbo (*University of Sannio*),
Stanislav Dashevskyi (*Forescout*), Daniel dos Santos (*Forescout*), Corrado Aaron Visaggio (*University of Sannio*)
- **Poster: DoHunter: A feature fusion-based LLM for DoH tunnel detection**..... 5012
Jiawen Diao (*Beijing Electronic Science and Technology Institute*),
Shengmin Zhao (*Beijing Electronic Science and Technology Institute*),
Jianguo Xie (*Beijing Electronic Science and Technology Institute*),
Rongna Xie (*Beijing Electronic Science and Technology Institute*),
Guozhen Shi (*Beijing Electronic Science and Technology Institute*)
- **Poster: From Fort to Foe: The Threat of RCE in RPKI** 5015
Oliver Jacobsen (*ATHENE & Goethe-Universität Frankfurt*),
Haya Schulmann (*ATHENE & Goethe-Universität Frankfurt*),
Niklas Vogel (*ATHENE & Goethe-Universität Frankfurt*),
Michael Waidner (*ATHENE & TU Darmstadt, & Fraunhofer SIT*)
- **Poster: Unmasking Label Errors: A need for Robust Cybersecurity Benchmarks**..... 5018
Shubham Malaviya (*TCS Research*), Manish Shukla (*TCS Research*), Saurabh Anand (*TCS Research*),
Sachin Lodha (*TCS Research*)
- **Poster: How Do Visually Impaired Users Navigate Accessibility Challenges in an Ad-Driven Web?**..... 5021
Abdul Haddi Amjad (*Virginia Tech*), Muhammad Ali Gulzar (*Virginia Tech*)
- **Poster: Automated Dependency Mapping for Web API Security Testing Using Large Language Models** 5024
Wanpeng Li (*University of Aberdeen*), Yuejun Guo (*Luxembourg Institute of Science and Technology*)
- **Poster: Acoustic Side-Channel Attack on Robot Vacuums** 5027
Peter Chen (*Virginia Tech*), Guannan Liu (*Colorado School of Mines*), Haining Wang (*Virginia Tech*)
- **Poster: Protecting Source Code Privacy When Hunting Bugs** 5030
Jielun Wu (*State Key Laboratory for Novel Software Technology, Nanjing University*),
Qingkai Shi (*State Key Laboratory for Novel Software Technology, Nanjing University*)
- **Poster: Enhancing Network Traffic Analysis with Pre-trained Side-channel Feature Imputation** 5033
Faqi Zhao (*Institute of Information Engineering; University of Chinese Academy of Sciences*),
Duohe Ma (*Institute of Information Engineering*),
Wenhao Li (*Research Institute of China Telecom Corporation Ltd.*),
Feng Liu (*Institute of Information Engineering*), Wen Wang (*Institute of Information Engineering*)
- **Poster: Protection against Source Inference Attacks in Federated Learning using Unary Encoding and Shuffling** 5036
Andreas Athanasiou (*INRIA and LIX, IPP*), Kangsoo Jung (*INRIA and LIX, IPP*),
Catuscia Palamidessi (*INRIA and LIX, IPP*)
- **Poster: FlashGuard: Real-time Disruption of Non-Price Flash Loan Attacks in DeFi** 5039
Abdulrahman Alhaidari (*Informatics and Networked Systems, University of Pittsburgh*),
Balaji Palanisamy (*Informatics and Networked Systems, University of Pittsburgh*),
Prashant Krishnamurthy (*Informatics and Networked Systems, University of Pittsburgh*)

- **Poster: Analyzing and Correcting Inaccurate CVE-CWE Mappings in the National Vulnerability Database** 5042
Şevval Şimşek (*Boston University*), Zhenpeng Shi (*Boston University*), Howell Xia (*Boston University*),
David Sastre Medina (*Red Hat Inc.*), David Starobinski (*Boston University*)
- **Poster: Solving the Free-rider Problem in Bittensor** 5045
Sin Tai Liu (*Opentensor Foundation*), Jiayuan Yu (*Information Systems Engineering, Concordia University*),
Jacob Steeves (*Opentensor Foundation*)
- **Poster: BlindMarket: A Trustworthy Chip Designs Marketplace for IP Vendors and Users** .. 5048
Zhaoxiang Liu (*Kansas State University*), Ning Luo (*UIUC*), Samuel Judson (*Yale University*),
Raj Gautam Dutta (*Silicon Assurance*), Xiaolong Guo (*Kansas State University*),
Mark Santolucito (*Barnard College, Columbia University*)
- **Poster: Security and Privacy Heterogeneous Environment for Reproducible Experimentation (SPHERE)**..... 5051
Jelena Mirkovic (*USC Information Sciences Institute*), David Balenson (*USC Information Sciences Institute*),
Brian Kocoloski (*USC Information Sciences Institute*), Geoff Lawler (*USC Information Sciences Institute*),
Chris Tran (*USC Information Sciences Institute*), Joseph Barnes (*USC Information Sciences Institute*),
Yuri Pradkin (*USC Information Sciences Institute*), Terry Benzel (*USC Information Sciences Institute*),
Srivatsan Ravi (*USC Information Sciences Institute*), Ganesh Sankaran (*USC Information Sciences Institute*),
Alba Regalado (*USC Information Sciences Institute*), David Choffnes (*Northeastern University*),
Daniel Dubois (*Northeastern University*), Luis Garcia (*University of Utah*)
- **Poster: Advanced Features for Real-Time Website Fingerprinting Attacks on Tor** 5054
Donghoon Kim (*Arkansas State University*), Andrew Booth (*Arkansas State University*),
Euijin Choo (*University of Alberta*), Doosung Hwang (*Dankook University*)
- **Poster: Byzantine Discrepancy Attacks against Calendar, Set-intersection and Nations** 5057
Yvo Desmedt (*Department of Computer Science, University of Texas at Dallas*),
Alireza Kavousi (*Department of Computer Science, University College London*),
Aydin Abadi (*School of Computing, Newcastle University*)
- **Poster: Enhance Hardware Domain Specific Large Language Model with Reinforcement Learning for Resilience** 5060
Weimin Fu (*Kansas State University*), Yifang Zhao (*University of Science and Technology of China*),
Yier Jin (*University of Science and Technology of China*), Xiaolong Guo (*Kansas State University*)
- **Poster: PGPNet: Classify APT Malware Using Prediction-Guided Prototype Network** 5063
Huafeng Bao (*Tencent*), Wenhao Li (*Research Institute of China Telecom Corporation Ltd*),
Zhaoxuan Li (*Institute of Information Engineering, Chinese Academy of Science*),
Han Miao (*Institute of Information Engineering, Chinese Academy of Science*),
Wen Wang (*Institute of Information Engineering, Chinese Academy of Science*),
Feng Liu (*Institute of Information Engineering, Chinese Academy of Science*)
- **Poster: Context-Based Effective Password Detection in Plaintext** 5066
Manish Shukla (*TCS Research*), Shubham Malaviya (*TCS Research*),
Sachin Lodha (*TCS Research*)
- **Poster: A Secure Multiparty Computation Platform for Squeaky-Clean Data Rooms**..... 5069
Pankaj Dayama (*IBM Research India*), Vinayaka Pandit (*IBM Research India*),
Sikhar Patranabis (*IBM Research India*), Abhishek Singh (*IBM Research India*),
Nitin Singh (*IBM Research India*)

Demonstration Session

- **Demo: Enhancing Smart Contract Security Comprehensively through Dynamic Symbolic Execution** 5072
Zhaoxuan Li (*Institute of Information Engineering, CAS & School of Cyber Security, UCAS*),
Ziming Zhao (*Zhejiang University*), Wenhao Li (*China Telecom Corp Ltd, Guangdong Research Institute*),
Rui Zhang (*Institute of Information Engineering, CAS*), Rui Xue (*Institute of Information Engineering, CAS*),
Siqu Lu (*Information Engineering University*), Fan Zhang (*Zhejiang University*)
- **Demo: FT-PrivacyScore: Personalized Privacy Scoring Service for Machine Learning Participation** 5075
Yuechun Gu (*UMBC*), Jiajie He (*UMBC*), Keke Chen (*UMBC*)

- **Demo: SGCode: A Flexible Prompt-Optimizing System for Secure Generation of Code** 5078
 Khiem Ton (*New Jersey Institute of Technology*), Nhi Nguyen (*New Jersey Institute of Technology*),
 Mahmoud Nazzal (*New Jersey Institute of Technology*), Abdallah Khreishah (*New Jersey Institute of Technology*),
 Cristian Borcea (*New Jersey Institute of Technology*), NhatHai Phan (*New Jersey Institute of Technology*),
 Ruoming Jin (*Kent State University*), Issa Khalil (*Qatar Computing Research Institute*),
 Yelong Shen (*Microsoft Azure AI*)
- **Demo: Towards Reproducible Evaluations of ML-Based IDS Using Data-Driven Approaches** 5081
 Solayman Ayoubi (*Sorbonne University, CNRS, LIP6*),
 Sébastien Tixeuil (*Sorbonne University, CNRS, LIP6 & Institut Universitaire de France*),
 Gregory Blanc (*SAMOVAR, Télécom SudParis Institut Polytechnique de Paris*),
 Houda Jmila (*Institute LIST, CEA, Paris-Saclay University*)
- **Demo: An End-to-End Anonymous Traffic Analysis System**..... 5084
 Huang Xianglan (*Southeast University*), Zhou Qiang (*Jiangsu University*),
 Wang Liangmin (*Southeast University*), Yu Weiqi (*Southeast University*),
 Wang Wenjin (*Southeast University*), Shen Shi (*Southeast University*)

Doctoral Symposium

- **ACM CCS 2024 Doctoral Symposium** 5087
 Gabriela Ciocarlie (*UT San Antonio*), Xinming Ou (*University of South Florida*)
- **Trusted Execution Environments for Quantum Computers** 5089
 Theodoros Trochatos (*Yale University*)
- **Towards Secure Runtime Auditing of Remote Embedded System Software**..... 5092
 Adam Caulfield (*Rochester Institute of Technology*)
- **Understanding and Addressing Online Tracking: Online Privacy’s Regulatory Turn** 5095
 Nathan Reitingner (*University of Maryland*)
- **Catch Me if You Can: Detecting Unauthorized Data Use in Training Deep Learning Models**..... 5098
 Zitao Chen (*The University of British Columbia*)
- **Evolving Network Security in the Era of Network Programmability** 5101
 Mingming Chen (*The Pennsylvania State University*)
- **Symbolic Execution for Dynamic Kernel Analysis**..... 5104
 Pansilu Pitigalaarachchi (*Singapore Management University*)
- **Toward Practical Threshold FHE: Low Communication, Computation and Interaction** 5107
 Hyeonmin Choe (*Department of Mathematical Science, Seoul National University*)
- **Privacy Analyses in Machine Learning** 5110
 Jiayuan Ye (*National University of Singapore*)
- **Novel Privacy Attacks and Defenses Against Neural Networks**..... 5113
 Sayanton V. Dibbo (*Dartmouth College*)
- **Leveraging Storage Semantics to Enhance Data Security and Privacy** 5116
 Weidong Zhu (*University of Florida*)
- **Securing Cyber-Physical Systems via Advanced Cyber Threat Intelligence Methods** 5119
 Efrén López-Morales (*Texas A&M University-Corpus Christi*)
- **Language-based Sandboxing** 5122
 Jialun Zhang (*Pennsylvania State University*)
- **Privacy-Preserving Graph Analysis** 5125
 Bhavish Raj Gopal (*Indian Institute of Science*)
- **Towards Proactive Protection against Unauthorized Speech Synthesis**..... 5128
 Zhiyuan Yu (*Washington University in St. Louis*)

2024 ACM CCS Organization

General Chairs: Bo Luo (*University of Kansas, USA*)
Xiaojing Liao (*Indiana University Bloomington, USA*)
Jun Xu (*University of Utah, USA*)

Program Chairs: Engin Kirda (*Northeastern University, USA*)
David Lie (*University of Toronto, Canada*)

Workshop Chairs: Christophe Hauser (*Dartmouth College, USA*)
Aurore Fass (*CISPA Helmholtz Center for Information Security, Germany*)

Poster/Demo Chairs: Sara Foresti (*Università degli Studi di Milano, Italy*)
Xiaoyan Sun (*Worcester Polytechnic Institute, USA*)

Artifact Evaluation Chair: Eric Eide (*University of Utah, USA*)

Doctoral Symposium Chairs: Xinming (Simon) Ou (*University of South Florida, USA*)
Gabriela F. Ciocarlie (*University of Texas at San Antonio, USA*)

Proceedings Chairs: Fengwei Zhang (*SUSTech, China*)
Dongpeng Xu (*University of New Hampshire, USA*)

Sponsorship Chairs: Kun Sun (*George Mason University, USA*)
Wendy Hui Wang (*Stevens Institute of Technology, USA*)

Travel Grant Chairs: Qi Li (*Tsinghua University, China*)
Adwait Nadkarni (*College of William & Mary, USA*)

Diversity, Equity, and Inclusion Betül Durak (*Microsoft Research, USA*)
Chairs: Fengjun Li (*University of Kansas, USA*)
Sophie Stephenson (*University of Wisconsin–Madison, USA*)

Publicity Chairs: Yang Zhang (*CISPA Helmholtz Center for Information Security, Germany*)
Kaitai Liang (*Delft University of Technology, Netherlands*)

Treasurer: Mu Zhang (*University of Utah, USA*)

Registration Chairs: Xueqiang Wang (*University of Central Florida, USA*)
Luis A. Garcia (*University of Utah, USA*)

Web Chairs: Yunhang Zhang (*University of Utah, USA*)
Xinda Wang (*University of Texas at Dallas, USA*)

Track Chairs: Yuan Tian (*UCLA, USA*)
Jason Polakis (*University of Illinois, USA*)
Aanjhan Ranganathan (*Northeastern University, USA*)
Catalin Hritcu (*MPI-SP, Germany*)
Yinqian Zhang (*SUSTech, China*)
Melek Onen (*Institut Eurecom, French*)
Katerina Mitrokotsa (*University of St. Gallen, Switzerland*)
Reza Shokri (*National University of Singapore, Singapore*)
Murat Kantarcioglu (*UT Dallas, USA*)
Blase Ur (*University of Chicago, USA*)
Gianluca Stringhini (*Boston University, USA*)
Stefanie Roos (*University of Kaiserslautern-Landau, Germany*)
Wouter Lueks (*CISPA, Germany*)

CCS 2024 Program Committee

Yousra Aafer (<i>University of Waterloo</i>)	Marcus Botacin (<i>Texas A&M University</i>)
Ali Abbasi (<i>CISPA Helmholtz Center for Information Security</i>)	Katharina Boudgoust (<i>CNRS</i>)
Reham Mohamed Aburas (<i>Purdue University</i>)	Ioana Boureanu (<i>University of Surrey</i>)
Sadia Afroz (<i>Gen Digital Inc</i>)	Anat Bremler Barr (<i>Tel Aviv University</i>)
Archita Agarwal (<i>MongoDB</i>)	Duc Bui (<i>Snap Inc.</i>)
Mohannad Alhanahnah (<i>University of Wisconsin Madison</i>)	Jeffrey Burdges (<i>Web 3.0 Technologies Foundation</i>)
Ghada Almashaqbeh (<i>University of Connecticut</i>)	Patricia Arias Cabarcos (<i>Paderborn University</i>)
Mário S. Alvim (<i>Universidade Federal de Minas Gerais - UFMG</i>)	Haipeng Cai (<i>Washington State University</i>)
Babak AminAzad (<i>Cloudflare</i>)	Yuandao Cai (<i>Huawei</i>)
Giovanni Apruzzese (<i>Liechtenstein Business School</i>)	Stefano Calzavara (<i>Università Ca' Foscari Venezia</i>)
Nalin Arachchilage (<i>University of Auckland</i>)	Matteo Campanelli (<i>Matter Labs</i>)
Héber H. Arcolezi (<i>Inria</i>)	Sébastien Canard (<i>Télécom Paris</i>)
Frederik Armknecht (<i>University of Mannheim</i>)	Javier Carnerero Cano (<i>IBM Research Europe/Imperial College London</i>)
Giuseppe Ateniese (<i>George Mason University</i>)	Yinzhi Cao (<i>Johns Hopkins University</i>)
Zeta Avarikioti (<i>TU Wien</i>)	Alvaro A. Cardenas (<i>University of California</i>)
Amro Awad (<i>North Carolina State University</i>)	Sergiu Carpov (<i>Inpher</i>)
Zhongjie Ba (<i>Zhejiang University</i>)	Ignacio Cascudo (<i>IMDEA Software Institute</i>)
Saikrishna Badrinarayanan (<i>LinkedIn</i>)	Lorenzo Cavallaro (<i>University College London</i>)
Eugene Bagdasaryan (<i>UMass / Google / Cornell</i>)	Z. Berkay Celik (<i>Purdue University</i>)
Guangdong Bai (<i>University of Queensland</i>)	Varun Chandrasekaran (<i>University of Wisconsin-Madison</i>)
Foteini Baldimtsi (<i>George Mason University</i>)	Urbi Chatterjee (<i>IIT Kanpur</i>)
Tiffany Bao (<i>Arizona State University</i>)	Ang Chen (<i>University of Michigan</i>)
Diogo Barradas (<i>University of Waterloo</i>)	Guoxing Chen (<i>Shanghai Jiao Tong University</i>)
Alexandre Bartel (<i>Umeå University (Sweden)</i>)	Huaming Chen (<i>The University of Sydney</i>)
Massimo Bartoletti (<i>University of Cagliari</i>)	Jianjun Chen (<i>Tsinghua University</i>)
Gabrielle Beck (<i>Johns Hopkins University</i>)	Jing Chen (<i>Tsinghua University</i>)
Alysson Bessani (<i>LASIGE</i>)	Kai Chen (<i>Institute of Information Engineering</i>)
Frédéric Besson (<i>Inria Rennes</i>)	Rongmao Chen (<i>National University of Defense Technology</i>)
Arjun Bhagoji (<i>University of Chicago</i>)	Sanchuan Chen (<i>Auburn University</i>)
Adithya Bhat (<i>Visa Research</i>)	Sen Chen (<i>Tianjin University</i>)
Pramod Bhatotia (<i>TU Munich</i>)	Weiteng Chen (<i>Microsoft Research</i>)
Eleanor Birrell (<i>Pomona College</i>)	Yanjiao Chen (<i>Zhejiang University</i>)
Bruno Blanchet (<i>Inria Paris</i>)	Yingying Chen (<i>Rutgers University</i>)
Erik-Oliver Blass (<i>Airbus</i>)	Long Cheng (<i>Clemson University</i>)
Olivier Blazy (<i>École Polytechnique</i>)	Albert Cheu (<i>Google Research</i>)
Jan Bobolz (<i>University of Edinburgh</i>)	James Hsin-yu Chiang (<i>Aarhus University</i>)
Franziska Boenisch (<i>CISPA</i>)	Tom Chotia (<i>University of Birmingham</i>)
Kevin Borgolte (<i>Ruhr University Bochum</i>)	Jeremy Clark (<i>Concordia University</i>)

Camille Cobb (*University of Illinois Urbana Champaign*)
Aisling Connolly (*DFINITY*)
Mauro Conti (*University of Padua*)
Jean-François Couchot (*Femto-ST Institute*)
Jedidiah R. Crandall (*Arizona State University*)
Cas Cremers (*CISPA Helmholtz Center for Information Security*)
Ana-Maria Cretu (*EPFL*)
Emiliano De Cristofaro (*UC Riverside*)
Daniele Cono D'Elia (*Sapienza University of Rome*)
Savino Dambra (*Norton Research Group*)
Anupam Das (*NC State*)
Debajyoti Das (*KU Leuven*)
Sourav Das (*University of Illinois at Urbana Champaign*)
Lucas Davi (*University of Duisburg-Essen*)
Alex Davidson (*Universidade NOVA de Lisboa*)
Jérémy Decouchant (*TU Delft*)
Stéphanie Delaune (*CNRS*)
Soteris Demetriou (*Imperial College London*)
Wenrui Diao (*Shandong University*)
Bolin Ding (*Alibaba Group*)
Yu Ding (*Google Research*)
Adam Doupe (*Arizona State University*)
Kostas Drakonakis (*University of Crete & FORTH*)
Dong Du (*Shanghai Jiao Tong University*)
Minxin Du (*Chinese University of Hong Kong*)
Sisi Duan (*Tsinghua University*)
Yue Duan (*Singapore Management University*)
Catherine Easdon (*Dynatrace Research*)
Manuel Egele (*Boston University*)
Thomas Eisenbarth (*University of Lübeck*)
Thorsten Eisenhofer (*TU Berlin*)
Tariq Elahi (*University of Edinburgh*)
Kaoutar Elkhayaoui (*IBM Research Zurich*)
Daniel Escudero (*J.P. Morgan AI Research*)
Muhammed F. Esgin (*Monash University*)
Vero Estrada (*EPFL*)
Dmitry Evtvushkin (*William & Mary*)
Ittay Eyal (*Technion*)
Song Fang (*University of Oklahoma*)
Antonio Faonio (*EURECOM*)
Oriol Farràs (*Universitat Rovira i Virgili*)
Habiba Farrukh (*University of California Irvine*)
Aurore Fass (*CISPA Helmholtz Center for Information Security*)
Hanwen Feng (*The University of Sydney*)
Yu Feng (*University of California*)
Ellis Fenske (*U.S. Naval Academy*)
Tobias Fiebig (*Max-Planck Institut for Informatics*)
Danilo Francati (*Aarhus University*)
Xinwen Fu (*University of Massachusetts Lowell*)
Benjamin Fuller (*University of Connecticut*)
Marco Gaboardi (*Boston University*)
Sébastien Gambs (*Université du Québec à Montréal*)
Carlos Gañán (*ICANN*)
Joshua Gancher (*CMU*)
Chaya Ganesh (*Indian Institute of Science*)
Peng Gao (*Virginia Tech*)
Xing Gao (*University of Delaware*)
Adria Gascon (*Google LLC*)
Peter Gazi (*IOG*)
Daniel Genkin (*Georgia Tech*)
Rosario Gennaro (*City College*)
Marilyn George (*Mongo DB*)
Arthur Gervais (*University College London & UC Berkeley RDI*)
Sepideh Ghanavati (*University of Maine*)
Mohammad Ghasemisharif (*Palo Alto Networks*)
Badih Ghazi (*Google*)
Nirnimesh Ghose (*University of Nebraska*)
Tom Van Goethem (*Google / KU Leuven*)
Oana Goga (*CNRS*)
Neil Gong (*Duke University*)
Devashish Gosain (*MPI-INF*)
Benjamin Gregoire (*Inria Sophia-Antipolis*)
Daniel Gruss (*Graz University of Technology*)
Guofei Gu (*Texas A&M*)
Le Guan (*University of Georgia*)
Marco Guarnieri (*IMDEA Software Institute*)
Zichen Gui (*ETH Zürich*)
Felix Günther (*IBM Research Europe – Zurich*)
Chuan Guo (*Meta*)
Jian Guo (*Nanyang Technological University*)
Shengjian (Daniel) Guo (*AWS Proactive Security*)

Wenbo Guo (<i>UCSB</i>)	Martin Johns (<i>TU Braunschweig</i>)
Emre Gursoy (<i>Koc University</i>)	Aaron Johnson (<i>US Naval Research Laboratory</i>)
Jun Han (<i>KAIST</i>)	Bailey Kacsmar (<i>University of Alberta</i>)
Lucjan Hanzlik (<i>CISPA Helmholtz Center for Information Security</i>)	Chris Kanich (<i>UIC</i>)
Jamie Hayes (<i>Deepmind</i>)	Murat Kantarcioglu (<i>UT Dallas</i>)
Weijia He (<i>Dartmouth College</i>)	Alexandros Kapravelos (<i>NCSU</i>)
Xi He (<i>University of Waterloo</i>)	Gabriel Kaptchuk (<i>Boston University</i>)
Ryan Henry (<i>University of Calgary</i>)	Ghassan Karame (<i>Ruhr University Bochum</i>)
Martin Henze (<i>RWTH Aachen University & Fraunhofer FKIE</i>)	Imtiaz Karim (<i>Purdue University</i>)
Stephen Herwig (<i>William & Mary</i>)	Harish Karthikeyan (<i>JPMorgan AI Research</i>)
Blaine Hoak (<i>University of Wisconsin-Madison</i>)	Ryan Kastner (<i>University of California</i>)
Daniel Holcomb (<i>UMass Amherst</i>)	Aniket Kate (<i>Purdue University / Supra Research</i>)
Geng Hong (<i>Fudan University</i>)	Jonathan Katz (<i>University of Maryland</i>)
Sanghyun Hong (<i>Oregon State University</i>)	Stefan Katzenbeisser (<i>University of Passau</i>)
Yuan Hong (<i>University of Connecticut</i>)	Marcel Keller (<i>CSIRO's Data61</i>)
Nicholas Hopper (<i>University of Minnesota</i>)	Vasileios Kemerlis (<i>Brown University</i>)
Kristina Hostakova (<i>ETH Zürich</i>)	Raouf Kerkouche (<i>The CISPA Helmholtz Center for Information Security</i>)
Amir Houmansadr (<i>UMass Amherst</i>)	Amin Kharraz (<i>Florida International University</i>)
Catalin Hritcu (<i>MPI-SP</i>)	Soheil Khodayari (<i>CISPA Helmholtz Center for Information Security</i>)
Justin Hsu (<i>Cornell University</i>)	Lucianna Kiffer (<i>ETH Zurich</i>)
Hong Hu (<i>The Pennsylvania State University</i>)	Sang Kil Cha (<i>KAIST</i>)
Hongxin Hu (<i>University at Buffalo</i>)	Doowon Kim (<i>University of Tennessee</i>)
Heqing Huang (<i>City University of Hong Kong</i>)	Taegyu Kim (<i>Pennsylvania State University</i>)
Wei Huang (<i>University of Toronto</i>)	Jakub Klemsa (<i>Zama</i>)
Zhen Huang (<i>De Paul University</i>)	Simon Koch (<i>Institute for Application Security (TU-Braunschweig)</i>)
Mathias Humbert (<i>University of Lausanne</i>)	Sebastian Köhler (<i>University of Oxford</i>)
Panagiotis Ilia (<i>Cyprus University of Technology</i>)	Katharina Kohls (<i>Ruhr University Bochum</i>)
Umar Iqbal (<i>Washington University in St. Louis</i>)	Lefteris Kokoris-Kogias (<i>IST Austria & Mysten Labs</i>)
Bahrz Jabiyev (<i>Dartmouth College</i>)	Chelsea H. Komlo (<i>University of Waterloo</i>)
Matthew Jagielski (<i>Google Research</i>)	Boris Köpf (<i>Azure Research</i>)
Suman Jana (<i>Columbia University</i>)	Kari Kostinen (<i>ETH Zurich</i>)
Kangkook Jee (<i>The University of Texas at Dallas</i>)	Adrien Koutsos (<i>Inria Paris</i>)
Yuseok Jeon (<i>UNIST</i>)	Stephan Krenn (<i>AIT Austrian Institute of Technology</i>)
Shouling Ji (<i>Zhejiang University</i>)	Deepak Kumar (<i>UC San Diego</i>)
Xiaoyu Ji (<i>Zhejiang University</i>)	Anil Kurmus (<i>IBM Research Europe - Zurich</i>)
Jinyuan Jia (<i>Penn State</i>)	Yonghwi Kwon (<i>University of Maryland</i>)
Limin Jia (<i>CMU</i>)	Pierre Laperdrix (<i>CNRS</i>)
Xiangkun Jia (<i>Institute of Software Chinese Academy of Sciences</i>)	Mario Larangeira (<i>IOHK</i>)
Yanxue Jia (<i>Purdue University</i>)	Peeter Laud (<i>Cybernetica AS</i>)
Yu Jiang (<i>Tsinghua University</i>)	Riccardo Lazzeretti (<i>Sapienza University of Rome</i>)

Duc Le (<i>Visa Research</i>)	Stefan Mangard (<i>Graz University of Technology</i>)
Tu Le (<i>UC Irvine</i>)	Michail Maniatakos (<i>NYU Abu Dhabi</i>)
Jaewoo Lee (<i>University of Georgia</i>)	Piotr Mardziel (<i>Independent</i>)
Hugo Lefeuvre (<i>The University of Manchester</i>)	Lenka Mareková (<i>ETH Zurich</i>)
Mohsen Lesani (<i>University of California</i>)	Luca Mariot (<i>University of Twente</i>)
Andrew Lewis-Pye (<i>London School of Economics</i>)	Evangelia Anna Markatou (<i>TU Delft</i>)
Jingjie Li (<i>University of Edinburgh</i>)	Daniel Masny (<i>Meta</i>)
Kang Li (<i>CertiK</i>)	Rahat Masood (<i>University of New South Wales</i>)
Mengyuan Li (<i>MIT</i>)	Elisaweta Masserova (<i>Carnegie Mellon University</i>)
Ming Li (<i>University of Texas</i>)	Ramya Masti (<i>Ampere Computing</i>)
Ming Li (<i>University Of Arizona</i>)	Ashraf Matrawy (<i>Carleton University</i>)
Qi Li (<i>Tsinghua University</i>)	Allison McDonald (<i>Boston University</i>)
Yuekang Li (<i>University of New South Wales</i>)	Stephen McQuistin (<i>University of St Andrews</i>)
Xiaojing Liao (<i>Indiana University Bloomington</i>)	Shagufta Mehnaz (<i>Penn State University</i>)
Xingwei Lin (<i>Ant Group</i>)	Guozhu Meng (<i>Institute of Information Engineering</i>)
Zhiqiang Lin (<i>Ohio State University</i>)	Wei Meng (<i>The Chinese University of Hong Kong</i>)
Chen Ling (<i>Boston University</i>)	Yan Meng (<i>Shanghai Jiao Tong University</i>)
Zhen Ling (<i>Southeast University</i>)	Sukarno Mertoguno (<i>Georgia Tech</i>)
Moritz Lipp (<i>Amazon Web Services</i>)	Samira Ajorpaz Mirbagher (<i>North Carolina State University</i>)
Alan Zaoxing Liu (<i>University of Maryland</i>)	Niloofar Miresghallah (<i>University of Washington</i>)
Jian Liu (<i>University of Tennessee</i>)	Omid Mirzaei (<i>Cisco Talos</i>)
Jinfei Liu (<i>Zhejiang University</i>)	Gargi Mitra (<i>University of British Columbia</i>)
Yang Liu (<i>NTU</i>)	Katerina Mitrokotsa (<i>University of St. Gallen</i>)
Zhuotao Liu (<i>Tsinghua University</i>)	Tarik Moataz (<i>MongoDB</i>)
Chen-Da Liu-Zhang (<i>Lucerne University of Applied Sciences and Arts & Web3 Foundation</i>)	Daniel Moghimi (<i>Google</i>)
Julian Loss (<i>CISPA Helmholtz Center for Information Security</i>)	Meisam Mohammady (<i>Iowa State University of Science and Technology</i>)
Jian Lou (<i>Zhejiang University</i>)	Atsuki Momose (<i>University of Illinois Urbana-Champaign</i>)
Yuan Lu (<i>Institute of Software Chinese Academy of Sciences</i>)	Mainack Mondal (<i>Indian Institute of Technology Kharagpur</i>)
Yun Lu (<i>University of Victoria</i>)	Tatsuya Mori (<i>Waseda University</i>)
Wouter Lueks (<i>CISPA</i>)	Giovane Moura (<i>SIDN Labs and TU Delft</i>)
Lannan Lisa Luo (<i>George Mason University</i>)	Pratyay Mukherjee (<i>Supra Research</i>)
Meng Luo (<i>Zhejiang University</i>)	Takao Murakami (<i>ISM</i>)
Xiapu Luo (<i>The Hong Kong Polytechnic University</i>)	Stefan Nagy (<i>University of Utah</i>)
Shiqing Ma (<i>University of Massachusetts Amherst</i>)	Yuhong Nan (<i>Sun Yat-sen University</i>)
Aravind Machiry (<i>Purdue University</i>)	Joseph Near (<i>University of Vermont</i>)
Matteo Maffei (<i>TU Wien</i>)	Benjamin Nguyen (<i>INSA Centre Val de Loire</i>)
Saeed Mahlouljifar (<i>Meta</i>)	Ngoc Khanh Nguyen (<i>King's College</i>)
Davide Maiorca (<i>University of Cagliari</i>)	Trung Tin Nguyen (<i>CISPA Helmholtz Center for Information Security</i>)
Eleftheria Makri (<i>LIACS at Leiden University</i>)	
Anna Maria Mandalari (<i>University College London</i>)	

Nick Nikiforakis (*Stony Brook University*)
 Kirill Nikitin (*Columbia University & New York Genome Center*)
 Valeria Nikolaenko (*A16Z Crypto Research*)
 Shirin Nilizadeh (*The University of Texas at Arlington*)
 Ryo Nishimaki (*NTT Social Informatics Laboratories*)
 Anca Nitulescu (*IOG*)
 Jianyu Niu (*Southern University of Science and Technology*)
 Mariusz Nowostawski (*Norwegian University of Science and Technology*)
 Olga Ohrimenko (*The University of Melbourne*)
 Hamed Okhravi (*MIT Lincoln Laboratory*)
 Oleksii Oleksenko (*Azure Research*)
 Ruxandra F. Olimid (*University of Bucharest*)
 Melek Onen (*EuroCom*)
 Cristina Onete (*University of Limoges/XLIM/CNRS 7252*)
 Michele Orrù (*University of Berkeley / Sorbonne University*)
 David Oswald (*University of Birmingham*)
 Simon Oya (*The University of British Columbia*)
 Tapas Pal (*NTT Corporation*)
 Catuscia Palamidessi (*Inria*)
 Balaji Palanisamy (*University of Pittsburgh*)
 Gaoning Pan (*Hangzhou Dianzi University*)
 Dimitrios Papadopoulos (*The Hong Kong University of Science and Technology*)
 Charalampos Papamanthou (*Yale University*)
 Pierre Parrend (*EPITA / University of Strasbourg*)
 Mathias Payer (*EPFL*)
 Roberto Perdisci (*University of Georgia*)
 Mert Pesé (*Clemson University*)
 Andreas Peter (*Carl von Ossietzky Universität Oldenburg*)
 Frank Piessens (*KU Leuven*)
 Benny Pinkas (*Aptos Labs*)
 Maura Pintor (*University of Cagliari*)
 Roger Piqueras Jover (*Google*)
 Sandeep Pisharody (*MIT Lincoln Labs*)
 Jason Polakis (*University of Illinois at Chicago*)
 Yuriy Polyakov (*Duality Technologies*)
 Dmitry Ponomarev (*Binghamton University*)
 Swarn Priya (*Virginia Tech*)
 Tobias Pulls (*Karlstad University*)
 Zhiyun Qian (*UC Riverside*)
 Kaihua Qin (*Yale University*)
 Zhan Qin (*Zhejiang University*)
 Syed Rafiul Hussain (*Pennsylvania State University*)
 Srinivasan Raghuraman (*Visa Research and MIT*)
 Aanjan Ranganathan (*Northeastern*)
 Nidhi Rastogi (*Rochester Institute of Technology*)
 Norrathep Rattanavipanon (*Prince of Songkla University*)
 Indrakshi Ray (*Colorado State University*)
 Kaveh Razavi (*ETH Zürich*)
 Joel Reardon (*University of Calgary*)
 Ling Ren (*University of Illinois at Urbana-Champaign*)
 Konrad Rieck (*TU Berlin*)
 Vera Rimmer (*KU Leuven*)
 Florentin Rochet (*University of Namur*)
 Stefanie Roos (*University of Kaiserslautern-Landau*)
 Walter Rudametkin (*IRISA / Inria / Univ. Rennes / IUF*)
 Alejandro Russo (*Chalmers University*)
 Rei Safavi-Naini (*University of Calgary*)
 Kazue Sako (*Waseda University*)
 Solmaz Salimi (*Eurecom*)
 Pedro Moreno Sanchez (*IMDEA Software Institute*)
 Iskander Sanchez-Rola (*Norton*)
 Vasily Sartakov (*Imperial College London*)
 Neetesh Saxena (*Cardiff University*)
 Stefan Schmid (*TU Berlin*)
 Guido Schmitz (*Lancaster University Leipzig*)
 Thomas Schneider (*TU Darmstadt*)
 Clara Schneidewind (*MPI-SP*)
 Lea Schönherr (*CISPA Helmholtz Center for Information Security*)
 Dominique Schröder (*Friedrich-Alexander Universität Erlangen-Nürnberg*)
 Michael Schwarz (*CISPA Helmholtz Center for Information Security*)
 Nader Sehatbakhsh (*UCLA*)
 Siamak F. Shahandashti (*University of York*)
 Filipo Sharevski (*DePaul University*)
 Saeed Sharifi-Malvajerdi (*Toyota Technological Institute at Chicago*)

Piyush Kumar Sharma (*University of Michigan*)
Dongdong She (*Hong Kong University of Science and Technology*)
Wenbo Shen (*Zhejiang University*)
Faysal Hossain Shezan (*University of Texas at Arlington*)
Qingkai Shi (*Nanjing University*)
Shweta Shinde (*ETH Zurich*)
Reza Shokri (*NUS*)
Ilia Shumailov (*Google Deepmind*)
Yan Shvartzshnaider (*York University*)
Amit Kumar Sikder (*Georgia Institute of Technology*)
Tjerand Silde (*Norwegian University of Science and Technology*)
Lucy Simko (*George Washington University*)
Mridula Singh (*CISPA*)
Daniel Slamanig (*Universität der Bundeswehr München*)
Georgios Smaragdakis (*Delft University of Technology*)
Alberto Sonnino (*Mysten Labs & University College London (UCL)*)
Claudio Soriente (*NEC Laboratories Europe*)
Alessandro Sorniotti (*IBM Research*)
Bas Spitters (*Aarhus University*)
Riccardo Spolaor (*Shandong University*)
Marco Squarcina (*TU Wien*)
Shravan Srinivasan (*Lagrange Labs*)
Cristian-Alexandru Staicu (*CISPA*)
Ben Stock (*CISPA Helmholtz Center for Information Security*)
Gianluca Stringhini (*Boston University*)
Thorsten Strufe (*Karlsruhe Institute of Technology*)
Min Suk Kang (*KAIST*)
Kun Sun (*George Mason University*)
Ruimin Sun (*Florida International University*)
Ruoxi Sun (*CSIRO's Data61*)
Wei Sun (*University of California San Diego*)
Petr Svenda (*Masaryk University*)
Marika Swanberg (*Boston University*)
Keisuke Tanaka (*Tokyo Institute of Technology*)
Qiang Tang (*Luxembourg Institute of Science and Technology (LIST)*)
Qiang Tang (*The University of Sydney*)

Zahra Tarkhani (*Microsoft*)
Vanessa Teague (*Thinking Cybersecurity*)
Erik Tews (*University of Twente*)
George Theodorakopoulos (*Cardiff University*)
Sri Aravinda Krishnan Thyagarajan (*University of Sydney*)
Yuan Tian (*UCLA*)
Nils Ole Tippenhauer (*CISPA Helmholtz Center for Information Security*)
Santiago Torres-Arias (*Purdue University*)
Muoi Tran (*ETH Zurich*)
Yiannis Tselekounis (*Royal Holloway*)
Hikaru Tsuchida (*NEC Corporation*)
Güliz Seray Tuncay (*Google*)
Fatih Turkmen (*University of Groningen*)
Benjamin Ujcich (*Georgetown University*)
Selcuk Uluagac (*Florida International University*)
Thomas Unterluggauer (*Intel labs*)
Blase Ur (*University of Chicago*)
Phani Vadrevu (*Louisiana State University*)
Mathy Vanhoef (*KU Leuven*)
Yash Vekaria (*University of California*)
Guru Venkataramani (*George Washington University*)
Alexios Voulimeneas (*Assistant Professor at TU Delft*)
Isabel Wagner (*University of Basel*)
Michael Waidner (*TU Darmstadt*)
Ryan Wails (*Georgetown University*)
Binghui Wang (*Illinois Institute of Technology*)
Di Wang (*King Abdullah University of Science and Technology*)
Gang Wang (*University of Illinois at Urbana-Champaign*)
Haoyu Wang (*Huazhong University of Science and Technology*)
Lingyu Wang (*Concordia University*)
Qichen Wang (*Hong Kong Baptist University*)
Ruoyu "Fish" Wang (*Arizona State University*)
Shangwen Wang (*National University of Defense Technology*)
Tao Wang (*Simon Fraser University*)
Tianhao Wang (*University of Virginia*)
Ting Wang (*Stony Brook University*)
Xuechao Wang (*HKUST(GZ)*)

Xueqiang Wang (<i>University of Central Florida</i>)	Fengwei Zhang (<i>Southern University of Science and Technology</i>)
Shiyi Wei (<i>University of Texas at Dallas</i>)	Haibin Zhang (<i>Yangtze Delta Region Institute of Tsinghua University</i>)
Rui Wen (<i>CISPA Helmholtz Center for Information Security</i>)	Hang Zhang (<i>Indiana University Bloomington</i>)
Chenkai Weng (<i>Northwestern University</i>)	Kehuan Zhang (<i>Chinese University of Hong Kong</i>)
Christian Wressnegger (<i>Karlsruhe Institute of Technology (KIT)</i>)	Lei Zhang (<i>Fudan University</i>)
Daoyuan Wu (<i>The Hong Kong University of Science and Technology</i>)	Mu Zhang (<i>University of Utah</i>)
Feng Wu (<i>University of Science and Technology of China</i>)	Ning Zhang (<i>Washington University in St. Louis</i>)
Tingmin Wu (<i>CSIRO's Data61</i>)	Ren Zhang (<i>Cryptape Co. Ltd. and Nervos</i>)
Karl Wüst (<i>Mysten Labs</i>)	Shufan Zhang (<i>University of Waterloo</i>)
Xiaokui Xiao (<i>NUS</i>)	Xiangyu Zhang (<i>Purdue University</i>)
Xusheng Xiao (<i>Arizona State University</i>)	Xiao Zhang (<i>CISPA Helmholtz Center for Information Security</i>)
Fengyuan Xu (<i>Nanjing University</i>)	Xiaokuan Zhang (<i>George Mason University</i>)
Xiaolin Xu (<i>Northeastern University</i>)	Yang Zhang (<i>CISPA Helmholtz Center for Information Security</i>)
Jason (Minhui) Xue (<i>CSIRO's Data61</i>)	Yinqian Zhang (<i>SUSTech</i>)
Qiben Yan (<i>MSU</i>)	Yuan Zhang (<i>Fudan University</i>)
Guangliang Yang (<i>Fudan University</i>)	Yue Zhang (<i>Drexel University</i>)
Kang Yang (<i>State Key Laboratory of Cryptology</i>)	Zaixi Zhang (<i>Harvard University</i>)
Yibin Yang (<i>Georgia Institute of Technology</i>)	Zhenkai Zhang (<i>Clemson University</i>)
Zheng Yang (<i>Georgia Institute of Technology</i>)	Zhikun Zhang (<i>Stanford & CISPA</i>)
Peisen Yao (<i>Zhejiang University</i>)	Zhuo Zhang (<i>Purdue University</i>)
Yaxing Yao (<i>Virginia Tech</i>)	Ben Y. Zhao (<i>University of Chicago</i>)
Zhihao (Zephyr) Yao (<i>New Jersey Institute of Technology</i>)	Binbin Zhao (<i>Georgia Institute of Technology</i>)
Jiayuan Ye (<i>National University of Singapore</i>)	Mang Zhao (<i>CISPA Helmholtz Center for Information Security</i>)
Michelle Yeo (<i>National University of Singapore</i>)	Qingchuan Zhao (<i>City University of Hong Kong</i>)
Wei You (<i>Renmin University of China</i>)	Ziming Zhao (<i>University at Buffalo</i>)
Chia-Mu Yu (<i>National Yang Ming Chiao Tung University</i>)	Hong-Sheng Zhou (<i>Virginia Commonwealth University</i>)
Jiangshan Yu (<i>The University of Sydney</i>)	Jie Zhou (<i>University of Rochester</i>)
Xin Yuan (<i>CSIRO's Data61</i>)	Yajin Zhou (<i>Zhejiang University</i>)
Stefano Zanero (<i>Politecnico di Milano</i>)	Ziqiao Zhou (<i>MSR Redmond</i>)
Savvas Zannettou (<i>TU Delft</i>)	Aviv Zohar (<i>Hebrew University of Jerusalem</i>)
Greg Zaverucha (<i>Microsoft Research</i>)	Saman Zonouz (<i>Georgia Tech</i>)
Qiang Zeng (<i>George Mason University</i>)	Yixin Zou (<i>Max Planck Institute for Security and Privacy</i>)
Fan Zhang (<i>Yale University</i>)	

CCS 2024 External Reviewers

Boladji Vinny Adjibi (*Georgia Institute of Technology*)
Fahmida Afrin (*University of Nebraska - Lincoln*)
Ayomide Akinsanya (*Stevens Institute of Technology*)
Manaar Alam (*New York University Abu Dhabi*)
Jannik Albrecht (*Ruhr University Bochum*)
Mohammed Alghazwi (*University of Groningen*)
Ghadeer Almusaddar (*Binghamton University*)
Seyed Behnam Andarzian (*Radboud University*)
Sebastien Andreina (*NEC Laboratories Europe*)
Vincenzo De Angelis (*University of Calabria*)
Md Sakib Anwar (*Ohio State University*)
Ananya Appan (*University of Illinois at Urbana-Champaign*)
Yeaseen Arafat (*University of Utah*)
Ali Arastehfard (*University of Connecticut*)
Marco Arazzi (*University of Pavia*)
Md Armanuzzaman (*University at Buffalo*)
Jessy Ayala (*University of California, Irvine*)
Ruben Baecker (*Friedrich-Alexander Universität Erlangen-Nürnberg*)
Shuangpeng Bai (*Penn State*)
Xuesong Bai (*University of California, Irvine*)
Patricia Guerra Balboa (*KIT/KASTEL*)
Akhil Bandrupalli (*Purdue University*)
Anaïs Barthoulot (*CNRS, Univ Montpellier, LIRMM, France*)
Enrico Bassetti (*Delft University of Technology*)
James Bell-Clark (*Google*)
Bruhadeshwar Bezawada (*Southern Arkansas University*)
Alexander Bienstock (*JPMorgan AI Research*)
Charlotte Bonte (*Zama*)
Tariq Bontekoe (*University of Groningen*)
Elijah Bouma-Sims (*Carnegie Mellon University*)
Andreas Brüggemann (*TU Darmstadt*)
Luis Burbano (*UC Santa Cruz*)
Claudio Canella (*Amazon Web Services*)
Sicong Cao (*Yangzhou University*)
Yiyue Cao (*Hong Kong University of Science and Technology (Guangzhou)*)
Diego Castejon-Molina (*IMDEA Software Institute*)

Sebastian Castro (*UC Santa Cruz*)
Stefano Cecconello (*University of Padova*)
Levent Çelik (*Clemson University*)
Gowri Chandran (*TU Darmstadt*)
Sylvain Chatel (*CISPA Helmholtz Center for Information Security*)
Chunjiang Che (*Hong Kong University of Science and Technology (Guangzhou)*)
Chen Chen (*Texas A&M University*)
Hanxiao Chen (*University of Electronic Science and Technology of China*)
Haobin Hiroki Chen (*Indiana University Bloomington*)
Jinrong Chen (*National University of Defense Technology*)
Shiyao Chen (*Nanyang Technological University*)
Xiangxiang Chen (*Zhejiang University*)
Yanju Chen (*University of California, Santa Barbara*)
Yihao Chen (*Tsinghua University*)
Yuntianyi Chen (*University of California, Irvine*)
Hao Cheng (*Institute of Software Chinese Academy of Sciences*)
Jiali Cheng (*National University of Defense Technology*)
Jiatao Cheng (*Sun Yat-sen University*)
Hien Chu (*TU Wien*)
Christoph Coijanovic (*KIT/KASTEL*)
Hao Cui (*University of California, Irvine*)
Hongrui Cui (*Shanghai Jiao Tong University*)
Jian Cui (*Indiana University Bloomington*)
Marc Damie (*University of Twente*)
Arash Daneshmand (*Concordia University*)
Priscilla Kyei Danso (*Stony Brook University*)
Xinhao Deng (*Tsinghua University*)
Amit Deo (*Zama*)
Arya Dharmaadi (*University of Groningen*)
Michalis Diamantaris (*Technical University of Crete*)
Aolin Ding (*Accenture Labs*)
Denis Donadel (*University of Padova*)
Tian Dong (*Shanghai Jiao Tong University*)
Andi Drebes (*Zama*)
Colin Drewes (*Stanford University*)

Alex Eastman (*University at Buffalo*)
 Kasra EdalatNejad (*TU Darmstadt*)
 Atefeh Mohseni Ejyeh (*University of California, Santa Barbara*)
 Mohamed Elshehaby (*Carleton University*)
 Alessandro Erba (*KIT, Karlsruhe*)
 Shuya Feng (*University of Connecticut*)
 Jean-Charles Noiro Ferrand (*University of Wisconsin-Madison*)
 Matthias Fitzi (*IOG*)
 Chuanpu Fu (*Tsinghua University*)
 Shaopeng Fu (*King Abdullah University of Science and Technology (KAUST)*)
 Tim Gellersen (*University of Lübeck*)
 Runpeng Geng (*Penn State*)
 Paul Gerhart (*TU Wien*)
 Lukas Gerlach (*CISPA Helmholtz Center for Information Security*)
 Diana Ghinea (*ETH Zurich*)
 Jens-Rene Giesen (*University of Duisburg-Essen*)
 Juanita Gomez (*UC Santa Cruz*)
 Tiantian Gong (*Purdue University*)
 Matt Gorbett (*Colorado State University*)
 Sanket Goutam (*Stony Brook University/Samsung Research America*)
 Xiaolan Gu (*University of Arizona*)
 Miquel Guiot (*Universitat Rovira i Virgili*)
 Daniel Günther (*Technical University of Darmstadt*)
 Jialong Guo (*Shandong University*)
 Xiaojie Guo (*Shanghai Qi Zhi Institute*)
 Mingda Han (*Shandong University*)
 Simon Hanisch (*TU Dresden*)
 Meng Hao (*Singapore Management University*)
 Dongnan He (*Renmin University of China*)
 Ningyu He (*Peking University*)
 Xu He (*George Mason University*)
 Yirui He (*University of California, Irvine*)
 Hasan Heydari (*LASIGE, FCUL, Univeristy of Lisbon*)
 Simeon Hoffmann (*CISPA*)
 Rayne Holland (*CSIRO's Data61*)
 Hanbin Hong (*University of Connecticut*)
 Florimond Houssiau (*Tune Insight SA*)
 Sabine Houy (*Umeå University*)

Bin Hu (*Beihang University*)
 Jingmei Hu (*Amazon*)
 Zhaojiie Hu (*University of Central Florida*)
 Liangyi Huang (*Arizona State University*)
 Qiqing Huang (*State University of New York at Buffalo*)
 Yuxi Huang (*Arizona State University*)
 Zhen Huang (*Shanghai Jiao Tong University*)
 Robin Hundt (*TU Darmstadt*)
 Mazharul Islam (*University of Wisconsin-Madison*)
 Vijayanta Jain (*University of Maine*)
 Zhiqiu Jiang (*CISPA Helmholtz Center for Information Security*)
 Wenqiang Jin (*Hunan University*)
 Zifeng Kang (*Johns Hopkins University*)
 Venkat Sai Suman Lamba Karanam (*University of Nebraska - Lincoln*)
 Khagan Karimov (*University of Utah*)
 Hugo Kermabon-Bobinnec (*Concordia University*)
 Nora Khayata (*TU Darmstadt*)
 Jung Hyun Kim (*KAIST*)
 Soomin Kim (*KAIST*)
 Jan H. Klemmer (*CISPA Helmholtz Center for Information Security*)
 Gihyuk Ko (*KAIST/Carnegie Mellon University*)
 Andreas Kogler (*Graz University of Technology*)
 Nishat Koti (*TU Darmstadt*)
 Julian Kotzur (*Friedrich-Alexander Universität Erlangen-Nürnberg*)
 Bruno Kreyssig (*Umeå University*)
 Joseph Lallemand (*Univ Rennes, CNRS, IRISA*)
 Hithem Lamri (*New York University Abu Dhabi*)
 Sara Lazzaro (*Mediterranea University of Reggio Calabria*)
 Jungwoo Lee (*KAIST*)
 Chaoqun Li (*Shandong University*)
 Haoxiang Li (*Renmin University of China*)
 Jichen Li (*Peking University*)
 Jingjie Li (*University of Edinburgh*)
 Kunyang Li (*University of Wisconsin-Madison*)
 Levi Taiji Li (*University of Utah*)
 Peiyang Li (*Tsinghua University*)
 Rui Li (*Shandong University*)
 Rujia Li (*Tsinghua University*)

Shuang Li (*Shandong University*)
 Weilin Li (*University College London*)
 Wenhao Li (*Shandong University*)
 Xingran Li (*Nanyang Technological University*)
 Yanan Li (*Univeristy of Sydney*)
 Ying Li (*University of California, Los Angeles*)
 Yu-De Lin (*CISPA*)
 Zilong Lin (*Indiana University Bloomington*)
 Eik List (*Nanyang Technological University*)
 Gaoxiang Liu (*University at Buffalo*)
 Han Liu (*Hong Kong University of Science and Technology*)
 Jing Liu (*University of California, Irvine/MPI-SP*)
 Junxu Liu (*The Hong Kong Polytechnic University*)
 Shuofeng Liu (*University of Queensland*)
 Song Liu (*Penn State*)
 Weiran Liu (*Alibaba Group*)
 Yinxi Liu (*The Chinese University of Hong Kong*)
 Yunpeng Liu (*Tsinghua University*)
 Zeyan Liu (*University of Kansas*)
 Zichen Liu (*Arizona State University*)
 Mengyi Long (*Sun Yat-sen University*)
 Stefano Longari (*Politecnico di Milano*)
 Juan Lozano (*UC Santa Cruz*)
 Shijie Lu (*Arizona State University*)
 Wen-jie LU (*Zhejiang University*)
 Nils Lukas (*Mohamed bin Zayed University of Artificial Intelligence (MBZUAI)*)
 Changhua Luo (*The Chinese University of Hong Kong*)
 Lin Ma (*Zhejiang University*)
 Shang Ma (*University of Notre Dame*)
 Zheyuan Ma (*University at Buffalo*)
 Zhongkui Ma (*University of Queensland*)
 Varun Madathil (*Yale University*)
 Dunia Mahboobeh (*New York University Abu Dhabi*)
 Yanmao Man (*HERE Technologies*)
 Neil Marchant (*The University of Melbourne*)
 Francesco Marchiori (*University of Padova*)
 Marcello Maugeri (*University of Catania*)
 Oleg Mazonka (*New York University Abu Dhabi*)
 Federico Mazzone (*University of Twente*)
 Nidà Meddouri (*EPITA Paris*)
 Sajad Meisami (*Illinois Institute of Technology*)
 Ying Meng (*George Mason University*)
 Julien Michel (*EPITA Strasbourg*)
 Phoebe Moh (*University of Maryland College Park*)
 Pedram MohajerAnsari (*Clemson University*)
 Malcom Mohamed (*Ruhr University Bochum*)
 Sareh Mohammadi (*Concordia University*)
 Logan Moody (*University of Virginia*)
 Hiraku Morita (*Aarhus University, Denmark*)
 Mir Imtiaz Mostafiz (*Purdue University*)
 Kazi Samin Mubasshir (*Purdue University*)
 Shaoor Munir (*University of California, Davis*)
 Alenkruth Krishnan Murali (*University of Virginia*)
 Mohammed Nabeel (*New York University Abu Dhabi*)
 Nima Naderloui (*University of Connecticut*)
 Rishub Nagpal (*Graz University of Technology*)
 Wenjie Nan (*Nanyang Technological University*)
 Jérôme Nguyen (*Universität der Bundeswehr München*)
 Tao Ni (*City University of Hong Kong*)
 Javier Nieto (*University of Illinois at Urbana-Champaign*)
 Pankaj Niroula (*William & Mary*)
 Momen Oqaily (*Concordia University*)
 David Paaßen (*University of Duisburg-Essen*)
 Derik Pack (*Clemson University*)
 Yu Pan (*University of Utah*)
 Christodoulos Pappas (*Hong Kong University of Science and Technology*)
 CheolJun Park (*Kyung Hee University*)
 Sangshin Park (*University of Utah*)
 Hannaneh B. Pasandi (*University of California, Berkeley*)
 Alex Miranda Pascual (*KIT/KASTEL*)
 Lorenzo Pisu (*University of Cagliari, Italy*)
 Mihail-Iulian Plesa (*University of Bucharest*)
 Daniel Pollman (*Lucerne University of Applied Sciences and Arts & ETH Zurich*)
 Sihang Pu (*CNRS, IRIF of Université Paris Cité*)
 Yuqi Qing (*Tsinghua University*)
 Anja Rabich (*University of Lübeck*)
 Imranur Rahman (*North Carolina State University*)
 Sebastian Ramacher (*AIT Austrian Institute of Technology*)
 Fabian Rauscher (*Graz University of Technology*)

Mathilde Raynal (*EPFL*)
 Nathan Reitinger (*University of Maryland*)
 Valentin Reyes Häusler (*University of Oldenburg*)
 Maryam Rezapour (*University of Connecticut*)
 Timothée Riom (*Umeå University*)
 Ritik Roongta (*New York University*)
 Miruna Rosca (*PiSquared*)
 Amir Salarpour (*Clemson University*)
 Jonas Sander (*University of Lübeck*)
 Alessandro Sanna (*University of Cagliari, Italy*)
 Silvia Lucia Sanna (*University of Cagliari, Italy*)
 Till Schlüter (*CISPA*)
 Christian Scholz (*University of Duisburg-Essen*)
 Shaila Sharmin (*International Islamic University Malaysia, Malaysia*)
 Xinyue Shen (*CISPA Helmholtz Center for Information Security*)
 Sachin Shukla (*Cisco Talos*)
 Gagandeep Singh (*University of Illinois Urbana-Champaign*)
 Diego Soi (*University of Cagliari, Italy*)
 Shang Song (*National University of Defense Technology*)
 Xiangfu Song (*National University of Singapore*)
 Vera Sosnovik (*University of Lausanne*)
 Ron Steinfeld (*Monash University*)
 Qiheng Sun (*Zhejiang University*)
 Yuqiang Sun (*Nanyang Technological University*)
 Nihal Talur (*UC Santa Cruz*)
 Louis Tremblay Thibault (*Zama*)
 M. Caner Tol (*Worcester Polytechnic Institute*)
 Cem Topcuoglu (*Northeastern University*)
 Anh-Duy Tran (*KU Leuven, Belgium*)
 Chris Tsoukaladelis (*Stony Brook University*)
 Billy Tsouvalas (*Stony Brook University*)
 Yu-Jye Tung (*University of California, Irvine*)
 Adithya Vadapalli (*IIT Kanpur*)
 Jayakrishna Menon Vadayath (*Arizona State University*)
 Nikhil Vanjani (*Carnegie Mellon University*)
 Christoforos Vasilatos (*New York University Abu Dhabi*)
 Robin Vassantlal (*LASIGE, FCUL, Univeristy of Lisbon*)

Caroline Violot (*University of Lausanne*)
 Easwar Vivek (*Supra Oracles*)
 Yann Vonlanthen (*ETH Zurich*)
 Michael Walter (*Zama*)
 Cheng-Long Wang (*KAUST*)
 Chenlin Wang (*The Chinese University of Hong Kong*)
 Chenyi Wang (*University of Arizona*)
 Guangjing Wang (*Michigan State University*)
 Huanting Wang (*University of Leeds*)
 Hulin Wang (*Arizona State University*)
 Junzhe Wang (*George Mason University*)
 Liu Wang (*Beijing University of Posts and Telecommunications*)
 Pei Wang (*Google*)
 Shen Wang (*Singapore Management University*)
 Xiaojian Wang (*North Carolina State University*)
 Yanting Wang (*Penn State*)
 Yi Wang (*National University of Defense Technology*)
 Yujie Wang (*Renmin University of China*)
 Zhipeng Wang (*Imperial College London*)
 Zihan Wang (*University of Queensland*)
 Zilun Wang (*The Chinese University of Hong Kong*)
 Ken Watanabe (*Waseda University*)
 Feng Wei (*State University of New York at Buffalo*)
 Haohuang Wen (*Ohio State University*)
 Vera Wesselkamp (*CISPA*)
 Annika Wilde (*Ruhr University Bochum*)
 Pascal Winkler (*University of Duisburg-Essen*)
 Jun Yeon Won (*Ohio State University*)
 Maverick Woo (*CMU*)
 Chuxiong Wu (*George Mason University*)
 Jiangrong Wu (*Sun Yat-sen University*)
 Yuexin Xiang (*Monash University*)
 Zihang Xiang (*KAUST*)
 Danning Xie (*Purdue University*)
 Dongchen Xie (*Renmin University of China*)
 Fuman Xie (*University of Queensland*)
 Shaoyuan Xie (*University of California, Irvine*)
 Jiajun Xin (*Hong Kong University of Science and Technology*)
 Haichuan Xu (*Georgia Institute of Technology*)
 Dan Yamamoto (*Internet Initiative Japan*)
 Chuan Yan (*University of Queensland*)

Jiaqin Yan (*Shanghai Jiao Tong University*)
Kailun Yan (*Shandong University*)
Shenao Yan (*University of Connecticut*)
Huanqi Yang (*City University of Hong Kong*)
Mengwei Yang (*University of California, Irvine*)
Shao Yang (*Case Western Reserve University*)
Shishuai Yang (*Shandong University*)
Yilong Yang (*University of Virginia*)
Yuqing Yang (*Ohio State University*)
Yuxin Yang (*Illinois Institute of Technology*)
Yingao “Elaine” Yao (*Cornell University*)
Mert Yassi (*Monash University*)
Hengkai Ye (*Penn State*)
Mingxi Ye (*Sun Yat-sen University*)
Qianyu Yu (*Hong Kong University of Science and Technology (Guangzhou)*)
Zheng Yu (*Northwestern University*)
Jiangfeng Yuan (*Renmin University of China*)
Tsz Hon Yuen (*Monash University*)
Shengfang Zhai (*Peking University*)
Zihao Zhan (*Texas Tech University*)
Bolin Zhang (*Hong Kong University of Science and Technology (Guangzhou)*)
Huaien Zhang (*The Hong Kong Polytechnic University*)
Jianting Zhang (*Purdue University*)

Jiayao Zhang (*Zhejiang University*)
Qifan Zhang (*University of California, Irvine*)
Xin Zhang (*Peking University*)
Xinyu Zhang (*Monash University*)
Yifan Zhang (*Vanderbilt University*)
Zhechang Zhang (*Penn State*)
Zicheng Zhang (*Singapore Management University*)
Zidong Zhang (*Shandong University*)
Qi Zhao (*Karlsruhe Institute of Technology (KIT)*)
Raymond K. Zhao (*CSIRO’s Data61*)
Shixuan Zhao (*Ohio State University*)
Yanjie Zhao (*Huazhong University of Science and Technology*)
Zheguang Zhao (*The University of Melbourne*)
Zijie Zhao (*University of Illinois Urbana-Champaign*)
Yu Zheng (*Chinese University of Hong Kong*)
Yusen Zheng (*Peking University*)
Huadi Zhu (*The University of Texas at Arlington*)
Xiaochen Zhu (*Massachusetts Institute of Technology*)
Zeying Zhu (*University of Maryland*)
Hui Zhuang (*Shandong University*)
Zeyang Zhuang (*The Chinese University of Hong Kong*)
Wei Zou (*Penn State*)
Noé Zufferey (*ETH Zurich*)

CCS 2024 Artifact Evaluation Committee

Boladji Vinny Adjibi (*Georgia Institute of Technology*)
Ayomide Akinsanya (*Stevens Institute of Technology*)
Ghadeer Almusaddar (*Binghamton University*)
Seyed Behnam Andarzian (*Radboud University*)
Yeaseen Arafat (*University of Utah*)
MD Armanuzzaman (*State University of New York at Buffalo*)
Jessy Ayala (*University of California, Irvine*)
Xuesong Bai (*University of California, Irvine*)
Elijah Bouma-Sims (*Carnegie Mellon University*)
Chen Chen (*Texas A&M University*)
Haobin Hiroki Chen (*Indiana University Bloomington*)
Yanju Chen (*University of California, Santa Barbara*)
Yuntianyi Chen (*University of California, Irvine*)
Hao Cui (*University of California, Irvine*)
Jian Cui (*Indiana University Bloomington*)
Priscilla Kyei Danso (*Stony Brook University*)
Vincenzo De Angelis (*University of Calabria*)
Xinhao Deng (*Tsinghua University*)
Aolin Ding (*Accenture Labs*)
Tian Dong (*Shanghai Jiao Tong University*)
Atefeh Mohseni Ejyeh (*University of California, Santa Barbara*)
Chuanpu Fu (*Tsinghua University*)
Shaopeng Fu (*King Abdullah University of Science and Technology (KAUST), Saudi Arabia*)
Lukas Gerlach (*CISPA Helmholtz Center for Information Security*)
Sanket Goutam (*Stony Brook University/Samsung Research America*)
Daniel Günther (*Technical University of Darmstadt*)
Mingda Han (*Shandong University*)
Ningyu He (*Peking University*)
Xu He (*George Mason University*)
Yirui He (*University of California, Irvine*)
Jingmei Hu (*Amazon*)
Qiqing Huang (*State University of New York at Buffalo*)
Mazharul Islam (*University of Wisconsin–Madison*)
Zifeng Kang (*Johns Hopkins University*)
Khagan Karimov (*University of Utah*)
Jung Hyun Kim (*KAIST*)
Jan H. Klemmer (*CISPA Helmholtz Center for Information Security*)
Gihyuk Ko (*KAIST/Carnegie Mellon University*)
Alenkruth Krishnan Murali (*University of Virginia*)
Sara Lazzaro (*Mediterranea University of Reggio Calabria*)
Chaoqun Li (*Shandong University*)
Levi Taiji Li (*University of Utah*)
Wenhao Li (*Shandong University*)
Ying Li (*University of California, Los Angeles*)
Zilong Lin (*Indiana University Bloomington*)
Jing Liu (*University of California, Irvine/MPI-SP*)
Zeyan Liu (*University of Kansas*)
Shijie Lu (*Arizona State University*)
Nils Lukas (*Mohamed bin Zayed University of Artificial Intelligence (MBZUAI)*)
Marcello Maugeri (*University of Catania*)
Ying Meng (*George Mason University*)
Phoebe Moh (*University of Maryland College Park*)
Logan Moody (*University of Virginia*)
Mir Imtiaz Mostafiz (*Purdue University*)
Kazi Samin Mubasshir (*Purdue University*)
Shaoor Munir (*University of California, Davis*)
Tao Ni (*City University of Hong Kong*)
Pankaj Niroula (*William & Mary*)
Yu Pan (*University of Utah*)
CheolJun Park (*Kyung Hee University*)
Sangshin Park (*University of Utah*)
Hannaneh B. Pasandi (*University of California, Berkeley*)
Imranur Rahman (*North Carolina State University*)
Nathan Reitinger (*University of Maryland*)
Maryam Rezapour (*University of Connecticut*)
Ritik Roongta (*New York University*)
Shaila Sharmin (*International Islamic University Malaysia, Malaysia*)
Xinyue Shen (*CISPA Helmholtz Center for Information Security*)
Xiangfu Song (*National University of Singapore*)
M. Caner Tol (*Worcester Polytechnic Institute*)
Anh-Duy Tran (*KU Leuven*)

Chris Tsoukaladelis (*Stony Brook University*)
Billy Tsouvalas (*Stony Brook University*)
Yu-Jye Tung (*University of California, Irvine*)
Adithya Vadapalli (*IIT Kanpur*)
Jayakrishna Menon Vadayath (*Arizona State University*)
Yann Vonlanthen (*ETH Zurich*)
Guangjing Wang (*Michigan State University*)
Huanting Wang (*University of Leeds*)
Hulin Wang (*Arizona State University*)
Junzhe Wang (*George Mason University*)
Liu Wang (*Beijing University of Posts and Telecommunications*)
Xiaojian Wang (*North Carolina State University*)
Zhipeng Wang (*Imperial College London*)
Feng Wei (*State University of New York at Buffalo*)
Chuxiong Wu (*George Mason University*)
Yuexin Xiang (*Monash University*)
Danning Xie (*Purdue University*)
Shaoyuan Xie (*University of California, Irvine*)
Haichuan Xu (*Georgia Institute of Technology*)
Kailun Yan (*Shandong University*)
Shenao Yan (*University of Connecticut*)
Huanqi Yang (*City University of Hong Kong*)

Mengwei Yang (*University of California, Irvine*)
Shao Yang (*Case Western Reserve University*)
Shishuai Yang (*Shandong University*)
Yilong Yang (*University of Virginia*)
Yingao “Elaine” Yao (*Cornell University*)
Mert Yassi (*Monash University*)
Zheng Yu (*Northwestern University*)
Shengfang Zhai (*Peking University*)
Huaien Zhang (*The Hong Kong Polytechnic University*)
Qifan Zhang (*University of California, Irvine*)
Xin Zhang (*Peking University*)
Yifan Zhang (*Vanderbilt University*)
Qi Zhao (*Karlsruhe Institute of Technology (KIT)*)
Raymond K. Zhao (*CSIRO's Data61*)
Yanjie Zhao (*Huazhong University of Science and Technology*)
Zijie Zhao (*University of Illinois Urbana-Champaign*)
Yu Zheng (*Chinese University of Hong Kong*)
Huadi Zhu (*The University of Texas at Arlington*)
Xiaochen Zhu (*Massachusetts Institute of Technology*)
Zeying Zhu (*University of Maryland*)
Hui Zhuang (*Shandong University*)
Noé Zufferey (*ETH Zurich*)

CCS 2024 Sponsor, Patrons, & Supporters

Sponsor:



Platinum
Patrons:



Gold
Patrons:



Gold
Patrons
(continued):



Silver
Patrons:



Bronze
Patrons:



Co-located
Event
Supporter:

