

November 26–30, 2023  
Copenhagen, Denmark



Association for  
Computing Machinery

*Advancing Computing as a Science & Profession*



# CCS '23

Proceedings of the 2023 ACM SIGSAC Conference on  
**Computer and Communications Security**

*Sponsored by:*

**ACM SIGSAC**

*General Chairs:*

**Weizhi Meng (Technical University of Denmark)**

**Christian D. Jensen (Technical University of Denmark)**

*Program Chairs:*

**Cas Cremers (CISPA Helmholtz Center for Information Security)**

**Engin Kirda (Khoury College of Computer Sciences)**



**Association for  
Computing Machinery**

*Advancing Computing as a Science & Profession*

**The Association for Computing Machinery**

**1601 Broadway, 10<sup>th</sup> Floor  
New York, NY 10019-7434**

**Copyright © 2023 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](mailto: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](http://www.copyright.com).

**ISBN: 979-8-4007-0050-7**

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](mailto:acmhelp@acm.org)

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

Printed in the USA

# Message from the ACM CCS 2023

## General Co-Chairs

On behalf of the ACM CCS 2023 Organizing Committee, we welcome you to the 30th ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM CCS continues to be the premier security 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.

This is the first time ACM CCS is held in Copenhagen Denmark, and we are happy to be back to a fully physical event after COVID-19. Copenhagen ranks high amongst the livable cities in the world and the size matches the national population of 6 million Danes. We like to think that the city is small, but still offers some of the urban metropolis vibe that is associated with capitals around the world. November in Denmark is the foundation of the Nordic noir genre of tv-series and detective novels, but despite the darkness and the inclement weather, we hope that you will explore the city and enjoy your stay in Copenhagen.

This year's main conference is one of the largest with 235 paper presentations over three days. We are also honored to have two distinguished keynote speakers for the main conference: Michael Reiter from Duke University (USA), and Lorrie Faith Craynor from Carnegie Mellon University (USA). In addition, fourteen workshops and one tutorial will take place on the pre-conference and post-conference days to discuss numerous specialized topics.

We are particularly thankful to the Program Chairs, Cas Cremers and Engin Kirda, the Track chairs, and all Program Committee members, as well as all the external reviewers, for their technical expertise and diligence to make an excellent technical program. We are thankful to our Workshop Chair (Jun Dai), the chairs of our co-located workshops and tutorials, and the workshop program committees, for assembling great workshop and tutorial programs. We express our gratitude to our organizing committee members: Publicity Chairs (Wenjuan Li and Rongxing Lu), Web Chairs (Wei-Yang Chiu and Brooke Lampe), Proceedings Chairs (Carter Yagemann and Emmanouil Vasilomanolakis), Sponsorship Chair (Bo Luo), Poster/Demo Chair (Sara Foresti), Student Travel Grant Chair (Jun Xu), and Artifact Evaluation Chair (Thorsten Holz). CCS 2023 would not have been possible without their devotion.

Furthermore, we would like to thank ACM and its Special Interest Group on Security, Audit and Control (SIGSAC) for their sponsorship of ACM CCS 2023. We offer our gratitude to our corporate sponsors for their generous support: Huawei, the National Science Foundation (NSF), Technology Innovation Institute (TII), Twenty-Second Century Dora Technology, Ant Research, IBM, TikTok, and Abelian.

Finally, we want to extend our gratitude to all the authors and volunteers for your involvement in ACM CCS 2023. It is you who make CCS a premier conference in Computer and Communications Security.

Sincerely,

ACM CCS 2023 General Chairs!

**Weizhi Meng**  
*Technical University of Denmark*

**Christian D. Jensen**  
*Technical University of Denmark*

# Welcome from the ACM CCS 2023

## Program Co-Chairs

Welcome to the proceedings of the 30th 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 May, each with a roughly 2.5-month review cycle. 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 engage in an interactive 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 440 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 ten Track Chairs: Leyla Bilge, Manuel Egele, Dario Fiore, Rob Jansen, Ghassan Karame, Steve Kremer, Veelasha Moonsamy, Nick Nikiforakis, Elissa Redmiles, and Selcuk Uluagac, 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 427 submissions, with 29 papers accepted (possibly with shepherding). An additional 48 papers were chosen for revision, with 47 of those eventually being accepted after the revised version was submitted. Of the papers that were rejected, 193 were rejected early. A total of 795 papers were submitted to the May cycle, with 90 papers accepted (possibly with shepherding) and 69 papers chosen to be revised. From the latter group, 68 papers were eventually accepted. Of the rejected papers, 367 were rejected early. Altogether, 235 out of 1222 submissions were accepted, for an acceptance rate of 19.15%. 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, Weizhi Meng and Christian D. Jensen, for organizing the conference, the Proceedings Chairs, Emmanouil Vasilomanolakis and Carter Yagemann, the Workshop Chair, Jun Dai, the Poster/Demo chair, Sara Foresti, 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!

**Cas Cremers**

*CISPA Helmholtz Center for Information Security*

**Engin Kirda**

*Khoury College of Computer Sciences*

# Table of Contents

CCS 2023 Conference Organization .....	xxviii
--	--------

CCS 2023 Sponsor & Supporters .....	xl
-------------------------------------	----

## Session 1: Cryptography for Anonymity

• <b>ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet</b> .....	1
Alexander Bienstock ( <i>New York University</i> ), Paul Rösler ( <i>FAU Erlangen-Nuremberg</i> ), Yi Tang ( <i>University of Michigan</i> )	
• <b>Lattice-Based Blind Signatures: Short, Efficient, and Round-Optimal</b> .....	16
Ward Beullens ( <i>IBM Research Europe - Zurich</i> ), Vadim Lyubashevsky ( <i>IBM Research Europe - Zurich</i> ), Ngoc Khanh Nguyen ( <i>EPFL</i> ), Gregor Seiler ( <i>IBM Research Europe - Zurich</i> )	
• <b>Aggregate Signatures with Versatile Randomization and Issuer-Hiding Multi-Authority Anonymous Credentials</b> .....	30
Omid Mir ( <i>Johannes Kepler University Linz</i> ), Balthazar Bauer ( <i>IRIF, Université de Paris Cité</i> ), Scott Griffy ( <i>Brown University</i> ), Anna Lysyanskaya ( <i>Brown University</i> ), Daniel Slamanig ( <i>AIT Austrian Institute of Technology</i> )	
• <b>Concurrent Security of Anonymous Credentials Light, Revisited</b> .....	45
Julia Kastner ( <i>ETH Zurich</i> ), Julian Loss ( <i>CISPA Helmholtz Center for Information Security</i> ), Omar Renawi ( <i>CISPA Helmholtz Center for Information Security, Saarland University</i> )	

## Session 2: Machine Learning Applications I

• <b>Decoding the Secrets of Machine Learning in Malware Classification: A Deep Dive into Datasets, Feature Extraction, and Model Performance</b> .....	60
Savino Dambra ( <i>Norton Research Group</i> ), Yufei Han ( <i>INRIA</i> ), Simone Aonzo ( <i>EURECOM</i> ), Platon Kotzias ( <i>Norton Research Group</i> ), Antonino Vitale ( <i>EURECOM</i> ), Juan Caballero ( <i>IMDEA Software Institute</i> ), Davide Balzarotti ( <i>EURECOM</i> ), Leyla Bilge ( <i>Norton Research Group</i> )	
• <b>Privacy Leakage via Speech-induced Vibrations on Room Objects through Remote Sensing based on Phased-MIMO</b> .....	75
Cong Shi ( <i>Rutgers University</i> ), Tianfang Zhang ( <i>Rutgers University</i> ), Zhaoyi Xu ( <i>Rutgers University</i> ), Shuping Li ( <i>Rutgers University</i> ), Donglin Gao ( <i>Rutgers University</i> ), Changming Li ( <i>Rutgers University</i> ), Athina Petropulu ( <i>Rutgers University</i> ), Chung-Tse Michael Wu ( <i>Rutgers University</i> ), Yingying Chen ( <i>Rutgers University</i> )	
• <b>Efficient Query-Based Attack against ML-Based Android Malware Detection under Knowledge Setting</b> .....	90
Ping He ( <i>Zhejiang University</i> ), Yifan Xia ( <i>Zhejiang University</i> ), Xuhong Zhang ( <i>Zhejiang University</i> ), Shouling Ji ( <i>Zhejiang University</i> )	
• <b>Your Battery Is a Blast! Safeguarding Against Counterfeit Batteries with Authentication</b> .....	105
Francesco Marchiori ( <i>University of Padova</i> ), Mauro Conti ( <i>University of Padova</i> )	

## Session 3: Attacks & Threats

• <b>TxPhishScope: Towards Detecting and Understanding Transaction-based Phishing on Ethereum</b> .....	120
Bowen He ( <i>Zhejiang University</i> ), Yuan Chen ( <i>Zhejiang University</i> ), Zhuo Chen ( <i>Zhejiang University</i> ), Xiaohui Hu ( <i>Beijing University of Posts and Telecommunications</i> ), Yufeng Hu ( <i>Zhejiang University</i> ), Lei Wu ( <i>Zhejiang University</i> ), Rui Chang ( <i>Zhejiang University</i> ), Haoyu Wang ( <i>Huazhong University of Science and Technology</i> ), Yajin Zhou ( <i>Zhejiang University</i> )	
• <b>Uncle Maker: (Time)Stamping Out The Competition in Ethereum</b> .....	135
Aviv Yaish ( <i>The Hebrew University</i> ), Gilad Stern ( <i>The Hebrew University</i> ), Aviv Zohar ( <i>The Hebrew University</i> )	

- **How Hard is Takeover in DPoS Blockchains? Understanding the Security of Coin-based Voting Governance** ..... 150  
Chao Li (*Beijing Jiaotong University*), Balaji Palanisamy (*University of Pittsburgh*),  
Runhua Xu (*Beihang University*), Li Duan (*Beijing Jiaotong University*),  
Jiqiang Liu (*Beijing Jiaotong University*), Wei Wang (*Beijing Jiaotong University*)
- **Demystifying DeFi MEV Activities in Flashbots Bundle** ..... 165  
Zihao Li (*The Hong Kong Polytechnic University*), Jianfeng Li (*Xi'an Jiaotong University*),  
Zheyuan He (*University of Electronic Science and Technology of China*),  
Xiapu Luo (*The Hong Kong Polytechnic University*), Ting Wang (*Pennsylvania State University*),  
Xiaozhe Ni (*University of Electronic Science and Technology of China*),  
Wenwu Yang (*University of Electronic Science and Technology of China*),  
Xi Chen (*University of Electronic Science and Technology of China*),  
Ting Chen (*University of Electronic Science and Technology of China*)

## Session 4: Usable Privacy

- **Marketing to Children Through Online Targeted Advertising: Targeting Mechanisms and Legal Aspects** ..... 180  
Tinhinane Medjkoune (*Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG*),  
Oana Goga (*LIX, CNRS, Inria, Ecole Polytechnique, Institut Polytechnique de Paris*),  
Juliette Senechal (*Universite de Lille, CRDP, DReDIS-IRJS*),
- **Pakistani Teens and Privacy - How Gender Disparities, Religion and Family Values Impact the Privacy Design Space**..... 195  
Maryam Mustafa (*Computer Science, Lahore University of Management Sciences*),  
Abdul Moeed Asad (*Purdue University*), Shehrbano Hassan (*Digital Rights Foundation*),  
Urooj Haider (*Computer Science, Lahore University of Management Sciences*),  
Zainab Durrani (*Digital Rights Foundation*),  
Katharina Krombholz (*CISPA Helmholtz Center for Information Security*)
- **Comprehension from Chaos: Towards Informed Consent for Private Computation**..... 210  
Bailey Kacsmar (*University of Alberta*), Vasisht Duddu (*University of Waterloo*),  
Kyle Tilbury (*University of Waterloo*), Blase Ur (*University of Chicago*),  
Florian Kerschbaum (*University of Waterloo*)
- **Privacy in the Age of Neurotechnology: Investigating Public Attitudes towards Brain Data Collection and Use** ..... 225  
Emiram Kablo (*Paderborn University*), Patricia Arias-Cabarcos (*Paderborn University*)

## Session 5: Side-Channels

- **Password-Stealing without Hacking: Wi-Fi Enabled Practical Keystroke Eavesdropping**..... 239  
Jingyang Hu (*Hunan University*), Hongbo Wang (*Nanyang Technological University*),  
Tianyue Zheng (*Nanyang Technological University*), Jingzhi Hu (*Nanyang Technological University*),  
Zhe Chen (*Fudan University*), Hongbo Jiang (*Hunan University*), Jun Luo (*Nanyang Technological University*)
- **Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel**..... 253  
Tao Ni (*City University of Hong Kong*), Xiaokuan Zhang (*George Mason University*),  
Qingchuan Zhao (*City University of Hong Kong*)
- **Optical Cryptanalysis: Recovering Cryptographic Keys from Power LED Light Fluctuations** ..... 268  
Ben Nassi (*Cornell Tech*), Ofek Vayner (*Ben-Gurion University of the Negev*),  
Etay Iluz (*Ben-Gurion University of the Negev*), Dudi Nassi (*Ben-Gurion University of the Negev*),  
Jan Jancar (*Masaryk University*), Daniel Genkin (*Georgia Tech*), Eran Tromer (*Boston University*),  
Boris Zadov (*Ben-Gurion University of the Negev*), Yuval Elovici (*Ben-Gurion University of the Negev*)
- **The Danger of Minimum Exposures: Understanding Cross-App Information Leaks on iOS through Multi-Side-Channel Learning** ..... 281  
Zihao Wang (*Indiana University Bloomington*), Jiale Guan (*Indiana University Bloomington*),  
XiaoFeng Wang (*Indiana University Bloomington*),  
Wenhao Wang (*Institute of Information Engineering, Chinese Academy of Sciences*),  
Luyi Xing (*Indiana University Bloomington*), Fares Alharbi (*Indiana University Bloomington*)

## Session 6: Cryptography & DNS

- **Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers** ..... 296  
Fenglu Zhang (*Tsinghua University*), Baojun Liu (*Tsinghua University*),  
Eihal Alowaisheq (*King Saud University*), Jianjun Chen (*Tsinghua University & Zhongguancun Laboratory*),  
Chaoyi Lu (*Tsinghua University*), Linjian Song (*Alibaba Group*), Yong Ma (*Alibaba Group*),  
Ying Liu (*Tsinghua University*), Haixin Duan (*Tsinghua University & Quancheng Laboratory*),  
Min Yang (*Fudan University*)
- **TSUKING: Coordinating DNS Resolvers and Queries into Potent DoS Amplifiers**..... 311  
Wei Xu (*Tsinghua University*), Xiang Li (*Tsinghua University*), Chaoyi Lu (*Tsinghua University*),  
Baojun Liu (*Tsinghua University*),  
Haixin Duan (*Tsinghua University & Quancheng Laboratory; Zhongguancun Laboratory*),  
Jia Zhang (*Tsinghua University & Zhongguancun Laboratory*),  
Jianjun Chen (*Tsinghua University & Zhongguancun Laboratory*), Tao Wan (*CableLabs*)
- **Under the Dark: A Systematical Study of Stealthy Mining Pools (Ab)use in the Wild**..... 326  
Zhenrui Zhang (*Tsinghua University & QI-ANXIN Technology Research Institute*),  
Geng Hong (*Fudan University*), Xiang Li (*Tsinghua University*), Zhuoqun Fu (*Tsinghua University*),  
Jia Zhang (*Tsinghua University & Zhongguancun Laboratory*),  
Mingxuan Liu (*Tsinghua University & Zhongguancun Laboratory*), Chuhan Wang (*Tsinghua University*),  
Jianjun Chen (*Tsinghua University & Zhongguancun Laboratory*),  
Baojun Liu (*Tsinghua University & Zhongguancun Laboratory*),  
Haixin Duan (*Tsinghua University & Quancheng Laboratory*),  
Chao Zhang (*Tsinghua University & Zhongguancun Laboratory*), Min Yang (*Fudan University*)
- **Travelling the Hypervisor and SSD: A Tag-Based Approach Against Crypto Ransomware with Fine-Grained Data Recovery** ..... 341  
Boyang Ma (*Xidian University*), Yilin Yang (*Xidian University*), Jinku Li (*Xidian University*),  
Fengwei Zhang (*Southern University of Science and Technology*), Wenbo Shen (*Zhejiang University*),  
Yajin Zhou (*Zhejiang University*), Jianfeng Ma (*Xidian University*)

## Session 7: Digital Signatures

- **Threshold Signatures from Inner Product Argument: Succinct, Weighted, and Multi-threshold**..... 356  
Sourav Das (*University of Illinois at Urbana-Champaign*), Philippe Camacho (*Espresso Systems*),  
Zhuolun Xiang (*Aptos Labs*), Javier Nieto (*University of Illinois at Urbana-Champaign*),  
Benedikt Bünz (*Espresso Systems*), Ling Ren (*University of Illinois at Urbana-Champaign*)
- **Post Quantum Fuzzy Stealth Signatures and Applications**..... 371  
Sihang Pu (*CISPA Helmholtz Center for Information Security*), Sri AravindaKrishnan Thyagarajan (*NTT Research*),  
Nico Döttling (*CISPA Helmholtz Center for Information Security*),  
Lucjan Hanzlik (*CISPA Helmholtz Center for Information Security*)
- **Chipmunk: Better Synchronized Multi-Signatures from Lattices**..... 386  
Nils Fleischhacker (*Ruhr University Bochum*), Gottfried Herold (*Ethereum Foundation*),  
Mark Simkin (*Ethereum Foundation*), Zhenfei Zhang (*Ethereum Foundation*)
- **AIM: Symmetric Primitive for Shorter Signatures with Stronger Security** ..... 401  
Seongkwang Kim (*Samsung SDS*), Jincheol Ha (*KAIST*), Mincheol Son (*KAIST*), Byeonghak Lee (*Samsung SDS*),  
Dukjae Moon (*Samsung SDS*), Joohee Lee (*Sungshin Women's University*), Sangyub Lee (*Samsung SDS*),  
Jihoon Kwon (*Samsung SDS*), Jihoon Cho (*Samsung SDS*), Hyojin Yoon (*Samsung SDS*), Jooyoung Lee (*KAIST*)

## Session 8: Machine Learning Applications II

- **FINER: Enhancing State-of-the-art Classifiers with Feature Attribution to Facilitate Security Analysis** ..... 416  
Yiling He (*Zhejiang University*), Jian Lou (*Zhejiang University*), Zhan Qin (*Zhejiang University*),  
Kui Ren (*Zhejiang University*)
- **Good-looking but Lacking Faithfulness: Understanding Local Explanation Methods through Trend-based Testing** ..... 431  
Jinwen He (*SKLOIS, IIE, CAS & School of Cyber Security, UCAS*),  
Kai Chen (*SKLOIS, IIE, CAS & School of Cyber Security, UCAS*),  
Guozhu Meng (*SKLOIS, IIE, CAS & School of Cyber Security, UCAS*),  
Jiangshan Zhang (*SKLOIS, IIE, CAS & School of Cyber Security, UCAS*),  
Congyi Li (*SKLOIS, IIE, CAS & School of Cyber Security, UCAS*)

- **FaceReader: Unobtrusively Mining Vital Signs and Vital Sign Embedded Sensitive Info via AR/VR Motion Sensors** ..... 446  
Tianfang Zhang (*Rutgers University*), Zhengkun Ye (*Temple University*),  
Ahmed Tanvir Mahdad (*Texas A&M University*), Md Mojibur Rahman Redoy Akanda (*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*)
- **AntiFake: Using Adversarial Audio to Prevent Unauthorized Speech Synthesis** ..... 460  
Zhiyuan Yu (*Washington University in St. Louis*), Shixuan Zhai (*Washington University in St. Louis*),  
Ning Zhang (*Washington University in St. Louis*)

## Session 9: Consensus Protocols

- **Themis: Fast, Strong Order-Fairness in Byzantine Consensus** ..... 475  
Mahimna Kelkar (*Cornell Tech*), Soubhik Deb (*University of Washington Seattle*), Sishan Long (*Cornell Tech*),  
Ari Juels (*Cornell Tech*), Sreeram Kannan (*University of Washington Seattle*)
- **Towards Practical Sleepy BFT** ..... 490  
Dahlia Malkhi (*Chainlink Labs*), Atsuki Momose (*University of Illinois at Urbana-Champaign*),  
Ling Ren (*University of Illinois at Urbana-Champaign*)
- **ParBFT: Faster Asynchronous BFT Consensus with a Parallel Optimistic Path** ..... 504  
Xiaohai Dai (*Huazhong University of Science and Technology*), Bolin Zhang (*Zhejiang University*),  
Hai Jin (*Huazhong University of Science and Technology*), Ling Ren (*University of Illinois at Urbana-Champaign*)
- **Abraxas: Throughput-Efficient Hybrid Asynchronous Consensus** ..... 519  
Erica Blum (*Reed College*), Jonathan Katz (*University of Maryland*),  
Julian Loss (*CISPA Helmholtz Center for Information Security*), Kartik Nayak (*Duke University*),  
Simon Ochsenreither (*Saarland University*)

## Session 10: Language-Based Security

- **Ou: Automating the Parallelization of Zero-Knowledge Protocols** ..... 534  
Yuyang Sang (*Yale University*), Ning Luo (*Northwestern University*), Samuel Judson (*Yale University*),  
Ben Chaimberg (*Yale University*), Timos Antonopoulos (*Yale University*), Xiao Wang (*Northwestern University*),  
Ruzica Piskac (*Yale University*), Zhong Shao (*Yale University*)
- **Black Ostrich: Web Application Scanning with String Solvers** ..... 549  
Benjamin Eriksson (*Chalmers University of Technology*), Amanda Stjerna (*Uppsala University*),  
Riccardo De Masellis (*Uppsala University*), Philipp Ruemmer (*University of Regensburg & Uppsala University*),  
Andrei Sabelfeld (*Chalmers University of Technology*)
- **Compars: Provably Secure Formats for Cryptographic Protocols** ..... 564  
Th  ophile Wallez (*Inria*), Jonathan Protzenko (*Microsoft Research*), Karthikeyan Bhargavan (*Inria and Cryspen*)

## Session 11: Quantum & Space

- **Exploration of Power Side-Channel Vulnerabilities in Quantum Computer Controllers** ..... 579  
Chuanqi Xu (*Yale University*), Ferhat Erata (*Yale University*), Jakub Szefer (*Yale University*)
- **Securing NISQ Quantum Computer Reset Operations Against Higher Energy State Attacks** ..... 594  
Chuanqi Xu (*Yale University*), Jessie Chen (*Yale University*), Allen Mi (*Yale University*),  
Jakub Szefer (*Yale University*)
- **Watch This Space: Securing Satellite Communication through Resilient Transmitter Fingerprinting** ..... 608  
Joshua Smailes (*University of Oxford*), Sebastian K  hler (*University of Oxford*),  
Simon Birnbach (*University of Oxford*), Martin Strohmeier (*armasuisse Science + Technology*),  
Ivan Martinovic (*University of Oxford*)
- **Protecting HRP UWB Ranging System Against Distance Reduction Attacks** ..... 622  
Kyungho Joo (*Korea University*), Dong Hoon Lee (*Korea University*), Yeonseon Jeong (*Korea University*),  
Wonsuk Choi (*Korea University*)

## Session 12: IoT: Attacks, Vulnerabilities, & Everything

- **BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses** ..... 636  
Daniele Antonioli (*EURECOM*)



- **When Free Tier Becomes Free to Enter: A Non-Intrusive Way to Identify Security Cameras with no Cloud Subscription** ..... 651  
Yan He (*The University of Oklahoma*), Qiuye He (*The University of Oklahoma*), Song Fang (*The University of Oklahoma*), Yao Liu (*University of South Florida*)
- **Formal Analysis of Access Control Mechanism of 5G Core Network** ..... 666  
Mujtahid Akon (*The Pennsylvania State University*), Tianchang Yang (*The Pennsylvania State University*), Yilu Dong (*The Pennsylvania State University*), Syed Rafiul Hussain (*The Pennsylvania State University*)
- **IoTFlow: Inferring IoT Device Behavior at Scale through Static Mobile Companion App Analysis** ..... 681  
David Schmidt (*TU Wien*), Carlotta Tagliaro (*TU Wien*), Kevin Borgolte (*Ruhr University Bochum*), Martina Lindorfer (*TU Wien*)

## Session 13: Homomorphic Encryption I

- **Homomorphic Multiple Precision Multiplication for CKKS and Reduced Modulus Consumption** ..... 696  
Jung Hee Cheon (*CryptoLab Inc. & Seoul National University*), Wonhee Cho (*Seoul National University*), Jaehyung Kim (*CryptoLab Inc.*), Damien Stehlé (*CryptoLab Inc.*)
- **PELTA - Shielding Multiparty-FHE against Malicious Adversaries** ..... 711  
Sylvain Chatel (*EPFL*), Christian Mouchet (*EPFL*), Ali Utkan Sahin (*EPFL*), Apostolos Pyrgelis (*EPFL*), Carmela Troncoso (*EPFL*), Jean-Pierre Hubaux (*EPFL*)
- **Asymptotically Faster Multi-Key Homomorphic Encryption from Homomorphic Gadget Decomposition** ..... 726  
Taechan Kim (*Samsung Research*), Hyesun Kwak (*Seoul National University*), Dongwon Lee (*Seoul National University*), Jinyeong Seo (*Seoul National University*), Yongsoo Song (*Seoul National University*)
- **FPT: A Fixed-Point Accelerator for Torus Fully Homomorphic Encryption** ..... 741  
Michiel Van Beirendonck (*COSIC, KU Leuven*), Jan-Pieter D'Anvers (*COSIC, KU Leuven*), Furkan Turan (*COSIC, KU Leuven*), Ingrid Verbauwhede (*COSIC, KU Leuven*)

## Session 14: Machine Learning Attacks I

- **Stolen Risks of Models with Security Properties** ..... 756  
Yue Qin (*Indiana University Bloomington*), Zhuoqun Fu (*Tsinghua University*), Chuyun Deng (*Tsinghua University*), Xiaojing Liao (*Indiana University Bloomington*), Jia Zhang (*Tsinghua University*), Haixin Duan (*Tsinghua University & Zhongguancun Laboratory*)
- **NARCISSUS: A Practical Clean-Label Backdoor Attack with Limited Information** ..... 771  
Yi Zeng (*Virginia Tech*), Minzhou Pan (*Virginia Tech*), Hoang Anh Just (*Virginia Tech*), Lingjuan Lyu (*Sony AI*), Meikang Qiu (*Augusta University*), Ruoxi Jia (*Virginia Tech*)
- **Stateful Defenses for Machine Learning Models Are Not Yet Secure Against Black-box Attacks** ..... 786  
Ryan Feng (*University of Michigan*), Ashish Hooda (*University of Wisconsin-Madison*), Neal Mangaokar (*University of Michigan*), Kassem Fawaz (*University of Wisconsin-Madison*), Somesh Jha (*University of Wisconsin-Madison*), Atul Prakash (*University of Michigan*)
- **Attack Some while Protecting Others: Selective Attack Strategies for Attacking and Protecting Multiple Concepts** ..... 801  
Vibha Belavadi (*University of Texas at Dallas*), Yan Zhou (*University of Texas at Dallas*), Murat Kantarcioglu (*University of Texas at Dallas*), Bhavani Thuraisingham (*University of Texas Dallas*)

## Session 15: Cryptographic Constructs & Models

- **FIN: Practical Signature-Free Asynchronous Common Subset in Constant Time** ..... 815  
Sisi Duan (*Tsinghua University*), Xin Wang (*Tsinghua University*), Haibin Zhang (*Beijing Institute of Technology*)
- **Analyzing the Real-World Security of the Algorand Blockchain** ..... 830  
Erica Blum (*Reed College*), Derek Leung (*Massachusetts Institute of Technology*), Julian Loss (*CISPA Helmholtz Center for Information Security*), Jonathan Katz (*University of Maryland*), Tal Rabin (*University of Pennsylvania*)

- **Fait Accompli Committee Selection: Improving the Size-Security Tradeoff of Stake-Based Committees** ..... 845  
Peter Gaži (IOG), Aggelos Kiayias (University of Edinburgh & IOG),  
Alexander Russell (University of Connecticut & IOG)
- **LedgerLocks: A Security Framework for Blockchain Protocols Based on Adaptor Signatures** ..... 859  
Erkan Tairi (TU Wien), Pedro Moreno-Sanchez (IMDEA Software Institute & Visa Research),  
Clara Schneidewind (MPI-SP)

## Session 16: Defenses

- **CAPACITY: Cryptographically-Enforced In-Process Capabilities for Modern ARM Architectures** ..... 874  
Kha Dinh Duy (Sungkyunkwan University), Kyuwon Cho (Sungkyunkwan University),  
Taehyun Noh (Sungkyunkwan University), Hojoon Lee (Sungkyunkwan University)
- **Cryptographically Enforced Memory Safety** ..... 889  
Martin Unterguggenberger (Graz University of Technology), David Schrammel (Graz University of Technology),  
Lukas Lamster (Graz University of Technology), Pascal Nasahl (Graz University of Technology),  
Stefan Mangard (Graz University of Technology)
- **Put Your Memory in Order: Efficient Domain-based Memory Isolation for WASM Applications** ..... 904  
Hanwen Lei (Peking University), Ziqi Zhang (Peking University), Shaokun Zhang (Peking University),  
Peng Jiang (Peking University), Zhineng Zhong (Peking University), Ningyu He (Peking University),  
Ding Li (Peking University), Yao Guo (Peking University), Xiangqun Chen (Peking University)
- **PANIC: PAN-assisted Intra-process Memory Isolation on ARM** ..... 919  
Jiali Xu (Institute of Computing Technology, CAS & University of Chinese Academy of Sciences),  
Mengyao Xie (Institute of Computing Technology, CAS & University of Chinese Academy of Sciences),  
Chenggang Wu (Institute of Computing Technology, CAS; University of Chinese Academy of Sciences; &  
Zhongguancun Laboratory),  
Yinqian Zhang (Department of Computer Science and Engineering, SUSTech & Research Institute of Trustworthy  
Autonomous Systems, SUSTech),  
Qijing Li (University of Chinese Academy of Sciences), Xuan Huang (Peking University),  
Yuanming Lai (Institute of Computing Technology, CAS & University of Chinese Academy of Sciences),  
Yan Kang (Institute of Computing Technology, CAS & University of Chinese Academy of Sciences),  
Wei Wang (Institute of Computing Technology, CAS),  
Qiang Wei (National Digital Switching System Engineering and Technological Research Center),  
Zhe Wang (Institute of Computing Technology, CAS; University of Chinese Academy of Sciences; & Zhongguancun  
Laboratory)

## Session 17: Secure Hardware

- **Security Verification of Low-Trust Architectures** ..... 945  
Qinhan Tan (Princeton University), Yonathan Fisseha (University of Michigan),  
Shibo Chen (University of Michigan), Lauren Biernacki (Lafayette College),  
Jean-Baptiste Jeannin (University of Michigan), Sharad Malik (Princeton University),  
Todd Austin (University of Michigan),
- **TunneLs for Bootlegging: Fully Reverse-Engineering GPU TLBs for Challenging Isolation Guarantees of NVIDIA MIG** ..... 960  
Zhenkai Zhang (Clemson University), Tyler Allen (University of North Carolina at Charlotte),  
Fan Yao (University of Central Florida), Xing Gao (University of Delaware), Rong Ge (Clemson University)
- **FetchBench: Systematic Identification and Characterization of Proprietary Prefetchers** ..... 975  
Till Schlüter (CISPA Helmholtz Center for Information Security),  
Amit Choudhari (CISPA Helmholtz Center for Information Security),  
Lorenz Hetterich (CISPA Helmholtz Center for Information Security),  
Leon Trampert (CISPA Helmholtz Center for Information Security),  
Hamed Nemati (CISPA Helmholtz Center for Information Security), Ahmad Ibrahim (Unaffiliated),  
Michael Schwarz (CISPA Helmholtz Center for Information Security),  
Christian Rossow (CISPA Helmholtz Center for Information Security),  
Nils Ole Tippenhauer (CISPA Helmholtz Center for Information Security)

- **Combined Private Circuits - Combined Security Refurbished** ..... 990  
Jakob Feldtkeller (*Ruhr University Bochum*), Tim Güneysu (*Ruhr University Bochum*),  
Thorben Moos (*Université catholique de Louvain*), Jan Richter-Brockmann (*Ruhr University Bochum*),  
Sayandeep Saha (*Université catholique de Louvain*), Pascal Sasdrich (*Ruhr University Bochum*),  
Francois-Xavier Standaert (*Université catholique de Louvain*)

## Session 18: Traffic Analysis

- **Point Cloud Analysis for ML-Based Malicious Traffic Detection: Reducing Majorities of False Positive Alarms** ..... 1005  
Chuanpu Fu (*Tsinghua University*), Qi Li (*Tsinghua University*), Ke Xu (*Tsinghua University*),  
Jianping Wu (*Tsinghua University*)
- **Learning from Limited Heterogeneous Training Data: Meta-Learning for Unsupervised Zero-Day Web Attack Detection across Web Domains** ..... 1020  
Peiyang Li (*Tsinghua University & BNRist*), Ye Wang (*Tsinghua University & BNRist*),  
Qi Li (*Tsinghua University*), Zhuotao Liu (*Tsinghua University*), Ke Xu (*Tsinghua University*),  
Ju Ren (*Tsinghua University*), Zhiying Liu (*Tencent*), Ruilin Lin (*Tencent*)
- **Realistic Website Fingerprinting By Augmenting Network Traces** ..... 1035  
Alireza Bahramali (*University of Massachusetts Amherst*),  
Ardavan Bozorgi (*University of Massachusetts Amherst*),  
Amir Houmansadr (*University of Massachusetts Amherst*)
- **Transformer-based Model for Multi-tab Website Fingerprinting Attack** ..... 1050  
Zhaoxin Jin (*Beijing University of Posts and Telecommunications & Ministry of Education*),  
Tianbo Lu (*Beijing University of Posts and Telecommunications & Ministry of Education*),  
Shuang Luo (*Beijing University of Posts and Telecommunications & Ministry of Education*),  
Jiaze Shang (*Beijing University of Posts and Telecommunications & Ministry of Education*)

## Session 19: Advanced Public Key Encryption

- **Efficient Registration-Based Encryption** ..... 1065  
Noemi Glaeser (*University of Maryland & Max Planck Institute for Security and Privacy*),  
Dimitris Kolonelos (*IMDEA Software Institute & Universidad Politécnica de Madrid*),  
Giulio Malavolta (*Bocconi University & Max Planck Institute for Security and Privacy*),  
Ahmadreza Rahimi (*Max Planck Institute for Security and Privacy*)
- **Efficient Set Membership Encryption and Applications** ..... 1080  
Matthew Green (*Johns Hopkins University*), Abhishek Jain (*Johns Hopkins University & NTT Research, Inc.*),  
Gijs Van Laer (*Johns Hopkins University & XFA.tech*)
- **Realizing Flexible Broadcast Encryption: How to Broadcast to a Public-Key Directory** ..... 1093  
Rachit Garg (*UT Austin*), George Lu (*UT Austin*), Brent Waters (*UT Austin & NTT Research*),  
David J. Wu (*UT Austin*)
- **Post-Quantum Multi-Recipient Public Key Encryption** ..... 1108  
Joël Alwen (*Amazon.com, Incorporated*), Dominik Hartmann (*Ruhr-Universität Bochum*),  
Eike Kiltz (*Ruhr-Universität Bochum*), Marta Mularczyk (*Amazon.com, Incorporated*),  
Peter Schwabe (*Max Planck Institute for Security and Privacy & Radboud University*)

## Session 20: Machine Learning Attacks II

- **Prediction Privacy in Distributed Multi-Exit Neural Networks: Vulnerabilities and Solutions** ..... 1123  
Tejas Kannan (*University of Chicago*), Nick Feamster (*University of Chicago*),  
Henry Hoffmann (*University of Chicago*)
- **Unforgeability in Stochastic Gradient Descent** ..... 1138  
Teodora Baluta (*National University of Singapore*), Ivica Nikolić (*National University of Singapore*),  
Rachit Jain (*National University of Singapore*), Divesh Aggarwal (*National University of Singapore*),  
Prateek Saxena (*National University of Singapore*)
- **Devil in Disguise: Breaching Graph Neural Networks Privacy through Infiltration** ..... 1153  
Lingshuo Meng (*Zhejiang University*), Yijie Bai (*Zhejiang University*), Yanjiao Chen (*Zhejiang University*),  
Yutong Hu (*Zhejiang University*), Wenyan Xu (*Zhejiang University*), Haiqin Weng (*Ant Group*)
- **Evading Watermark based Detection of AI-Generated Content** ..... 1168  
Zhengyuan Jiang (*Duke University*), Jinghui Zhang (*Duke University*), Neil Zhenqiang Gong (*Duke University*)

## Session 21: Defenses & Smart Contract Security

- **Phoenix: Detect and Locate Resilience Issues in Blockchain via Context-Sensitive Chaos** .... 1182  
Fuchen Ma (*Tsinghua University*), Yuanliang Chen (*Tsinghua University*), Yuanhang Zhou (*Tsinghua University*),  
Jingxuan Sun (*Beijing University of Posts and Telecommunications*), Zhuo Su (*Tsinghua University*),  
Yu Jiang (*Tsinghua University*), Jianguang Sun (*Tsinghua University*), Huizhong Li (*WeBank*)
- **Fuzz on the Beach: Fuzzing Solana Smart Contracts** ..... 1197  
Sven Smolka (*University of Duisburg-Essen*), Jens-Rene Giesen (*University of Duisburg-Essen*),  
Pascal Winkler (*University of Duisburg-Essen*), Oussama Draissi (*University of Duisburg-Essen*),  
Lucas Davi (*University of Duisburg-Essen*), Ghassan Karamé (*Ruhr University Bochum*),  
Klaus Pohl (*University of Duisburg-Essen*)
- **Lanturn: Measuring Economic Security of Smart Contracts Through Adaptive Learning** .... 1212  
Kushal Babel (*Cornell Tech & IC3*), Mojan Javaheripi (*University of California San Diego*),  
Yan Ji (*Cornell Tech & IC3*), Mahimna Kelkar (*Cornell Tech & IC3*),  
Farinaz Koushanfar (*University of California San Diego*), Ari Juels (*Cornell Tech & IC3*)
- **Riggs: Decentralized Sealed-Bid Auctions** ..... 1227  
Nirvan Tyagi (*Cornell University*), Arasu Arun (*New York University*), Cody Freitag (*Cornell Tech*),  
Riad Wahby (*Carnegie Mellon University*), Joseph Bonneau (*New York University*), David Mazières (*Stanford University*)

## Session 22: Fuzzing I

- **DSFuzz: Detecting Deep State Bugs with Dependent State Exploration** ..... 1242  
Yinxi Liu (*The Chinese University of Hong Kong*), Wei Meng (*The Chinese University of Hong Kong*)
- **Profile-guided System Optimizations for Accelerated Greybox Fuzzing** ..... 1257  
Yunhang Zhang (*University of Utah*), Chengbin Pang (*Nanjing University*), Stefan Nagy (*University of Utah*),  
Xun Chen (*Samsung Research America*), Jun Xu (*University of Utah*)
- **NESTFUZZ: Enhancing Fuzzing with Comprehensive Understanding of Input Processing Logic** ..... 1272  
Peng Deng (*Fudan University*), Zhemin Yang (*Fudan University*), Lei Zhang (*Fudan University*),  
Guangliang Yang (*Fudan University*), Wenzheng Hong (*Fudan University*), Yuan Zhang (*Fudan University*),  
Min Yang (*Fudan University*)
- **Lifting Network Protocol Implementation to Precise Format Specification with Security Applications** ..... 1287  
Qingkai Shi (*Purdue University*), Junyang Shao (*Purdue University*), Yapeng Ye (*Purdue University*),  
Mingwei Zheng (*Purdue University*), Xiangyu Zhang (*Purdue University*)

## Session 23: IoT & Embedded Security

- **MicPro: Microphone-based Voice Privacy Protection** ..... 1302  
Shilin Xiao (*Zhejiang University*), Xiaoyu Ji (*Zhejiang University*), Chen Yan (*Zhejiang University*),  
Zhicong Zheng (*Zhejiang University*), Wenyan Xu (*Zhejiang University*)
- **TileMask: A Passive-Reflection-based Attack against mmWave Radar Object Detection in Autonomous Driving** ..... 1317  
Yi Zhu (*University at Buffalo, the State University of New York*), Chenglin Miao (*Iowa State University*),  
Hongfei Xue (*University of North Carolina at Charlotte*), Zhengxiong Li (*University of Colorado Denver*),  
Yunnan Yu (*University at Buffalo, the State University of New York*),  
Wenyao Xu (*University at Buffalo, the State University of New York*), Lu Su (*Purdue University*),  
Chunming Qiao (*University at Buffalo, the State University of New York*)
- **SHERLOC: Secure and Holistic Control-Flow Violation Detection on Embedded Systems** ... 1332  
Xi Tan (*University at Buffalo*), Ziming Zhao (*University at Buffalo*)
- **Caveat (IoT) Emptor: Towards Transparency of IoT Device Presence** ..... 1347  
Sashidhar Jakkamsetti (*University of California, Irvine*), Youngil Kim (*University of California, Irvine*),  
Gene Tsudik (*University of California, Irvine*)

## Session 24: Formal Analysis of Cryptographic Protocols

- **CRYPTOBAP: A Binary Analysis Platform for Cryptographic Protocols** ..... 1362  
Faezeh Nasrabadi (*CISPA Helmholtz Center for Information Security*),  
Robert Künnemann (*CISPA Helmholtz Center for Information Security*),  
Hamed Nematì (*CISPA Helmholtz Center for Information Security*)

- **A Generic Methodology for the Modular Verification of Security Protocol Implementations** ..... 1377  
Linard Arquint (*ETH Zurich*), Malte Schwerhoff (*ETH Zurich*), Vaibhav Mehta (*Cornell University*), Peter Müller (*ETH Zurich*)
- **Provably Unlinkable Smart Card-based Payments**..... 1392  
Sergiu Bursuc (*University of Luxembourg*), Ross Horne (*University of Luxembourg & University of Strathclyde*), Sjouke Mauw (*University of Luxembourg*), Semen Yurkov (*University of Luxembourg*)
- **CHECKMATE: Automated Game-Theoretic Security Reasoning**..... 1407  
Lea Salome Brugger (*ETH Zurich*), Laura Kovács (*TU Wien*), Anja Petković Komel (*TU Wien*), Sophie Rain (*TU Wien*), Michael Rawson (*TU Wien*)

## Session 25: Zero Knowledge Proofs

- **Recursion over Public-Coin Interactive Proof Systems; Faster Hash Verification** ..... 1422  
Alexandre Belling (*Consensys, Linea*), Azam Soleimanian (*Consensys, Linea*), Olivier Bégassat (*Consensys, Linea*)
- **Modular Sumcheck Proofs with Applications to Machine Learning and Image Processing** . 1437  
David Balbás (*IMDEA Software Institute & Universidad Politécnica de Madrid*), Dario Fiore (*IMDEA Software Institute*), Maria Isabel González Vasco (*Universidad Carlos III de Madrid*), Damien Robissout (*IMDEA Software Institute*), Claudio Soriente (*NEC Laboratories Europe*)
- **Batchman and Robin: Batched and Non-batched Branching for Interactive ZK** ..... 1452  
Yibin Yang (*Georgia Institute of Technology*), David Heath (*University of Illinois Urbana-Champaign*), Carmit Hazay (*Bar-Ilan University*), Vladimir Kolesnikov (*Georgia Institute of Technology*), Muthuramakrishnan Venkitasubramaniam (*Ligero Inc.*)
- **Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions** ..... 1467  
Diego F. Aranha (*Aarhus University*), Carsten Baum (*DTU Copenhagen*), Kristian Gjøsteen (*Norwegian University of Science and Technology*), Tjerdand Silde (*Norwegian University of Science and Technology*)

## Session 26: Federated Learning

- **Turning Privacy-preserving Mechanisms against Federated Learning** ..... 1482  
Marco Arazzi (*University of Pavia*), Mauro Conti (*University of Padua & Delft University of Technology*), Antonino Nocera (*University of Pavia*), Stjepan Picek (*Radboud University & Delft University of Technology*)
- **martFL: Enabling Utility-Driven Data Marketplace with a Robust and Verifiable Federated Learning Architecture**..... 1496  
Qi Li (*Tsinghua University & Zhongguancun Laboratory*), Zhuotao Liu (*Tsinghua University & Zhongguancun Laboratory*), Qi Li (*Tsinghua University & Zhongguancun Laboratory*), Ke Xu (*Tsinghua University & Zhongguancun Laboratory*)
- **Unraveling the Connections between Privacy and Certified Robustness in Federated Learning Against Poisoning Attacks**..... 1511  
Chulin Xie (*University of Illinois at Urbana-Champaign*), Yunhui Long (*University of Illinois at Urbana-Champaign*), Pin-Yu Chen (*IBM Research*), Qinbin Li (*UC Berkeley*), Sanmi Koyejo (*Stanford University*), Bo Li (*University of Illinois at Urbana-Champaign*)
- **MESAS: Poisoning Defense for Federated Learning Resilient against Adaptive Attackers**.... 1526  
Torsten Krauß (*University of Würzburg*), Alexandra Dmitrienko (*University of Würzburg*)

## Session 27: Interoperability & 2nd Layer Solutions

- **Accio: Variable-Amount, Optimized-Unlinkable and NIZK-Free Off-Chain Payments via Hubs**..... 1541  
Zhonghui Ge (*Shanghai Jiao Tong University*), Jiayuan Gu (*Shanghai Jiao Tong University*), Chenke Wang (*Shanghai Jiao Tong University*), Yu Long (*Shanghai Jiao Tong University*), Xian Xu (*East China University of Science and Technology*), Dawu Gu (*Shanghai Jiao Tong University*)
- **CryptoConcurrency: (Almost) Consensusless Asset Transfer with Shared Accounts**..... 1556  
Andrei Tonkikh (*Télécom Paris, Institut Polytechnique de Paris*), Pavel Ponomarev (*Georgia Institute of Technology*), Petr Kuznetsov (*Télécom Paris, Institut Polytechnique de Paris*), Yvonne-Anne Pignolet (*DFINITY*)

- **TrustBoost: Boosting Trust among Interoperable Blockchains**..... 1571  
Peiyao Sheng (*University of Illinois Urbana-Champaign*),  
Xuechao Wang (*The Hong Kong University of Science and Technology (Guangzhou)*),  
Sreeram Kannan (*University of Washington*), Kartik Nayak (*Duke University*),  
Pramod Viswanath (*Princeton University*)
- **Interchain Timestamping for Mesh Security** ..... 1585  
Ertem Nusret Tas (*Stanford University*), Runchao Han (*BabylonChain*), David Tse (*Stanford University*),  
Mingchao Yu (*BabylonChain*)

## Session 28: Fuzzing II

- **HOPPER: Interpretative Fuzzing for Libraries**..... 1600  
Peng Chen (*Tencent Security Big Data Lab*), Yuxuan Xie (*Tencent Security Big Data Lab*),  
Yunlong Lyu (*Tencent Security Big Data Lab*), Yuxiao Wang (*Tencent Security Big Data Lab*),  
Hao Chen (*University of California, Davis*)
- **Greybox Fuzzing of Distributed Systems** ..... 1615  
Ruijie Meng (*National University of Singapore*), George Pirlea (*National University of Singapore*),  
Abhik Roychoudhury (*National University of Singapore*), Ilya Sergey (*National University of Singapore*)
- **SYZDIRECT: Directed Greybox Fuzzing for Linux Kernel**..... 1630  
Xin Tan (*Fudan University*), Yuan Zhang (*Fudan University*), Jiadong Lu (*Fudan University*),  
Xin Xiong (*Fudan University*), Zhuang Liu (*Fudan University*), Min Yang (*Fudan University*)
- **PyRTFUZZ: Detecting Bugs in Python Runtimes via Two-Level Collaborative Fuzzing**..... 1645  
Wen Li (*Washington State University*), Haoran Yang (*Washington State University*),  
Xiapu Luo (*The Hong Kong Polytechnic University*), Long Cheng (*Clemson University*),  
Haipeng Cai (*Washington State University*)

## Session 29: Cryptography & Side-Channels

- **FITS: Matching Camera Fingerprints Subject to Software Noise Pollution** ..... 1660  
Liu Liu (*Zhejiang University & Jiaxing Research Institute, Zhejiang University*),  
Xinwen Fu (*University of Massachusetts Lowell*),  
Xiaodong Chen (*Zhejiang University & Jiaxing Research Institute, Zhejiang University*),  
Jianpeng Wang (*Zhejiang University & Jiaxing Research Institute, Zhejiang University*),  
Zhongjie Ba (*Zhejiang University & Jiaxing Research Institute, Zhejiang University*),  
Feng Lin (*Zhejiang University & Jiaxing Research Institute, Zhejiang University*),  
Li Lu (*Zhejiang University & Jiaxing Research Institute, Zhejiang University*),  
Kui Ren (*Zhejiang University & Jiaxing Research Institute, Zhejiang University*)
- **LeakyOhm: Secret Bits Extraction using Impedance Analysis** ..... 1675  
Saleh Khalaj Monfared (*Worcester Polytechnic Institute*), Tahoura Mosavirik (*Worcester Polytechnic Institute*),  
Shahin Tajik (*Worcester Polytechnic Institute*)
- **A Systematic Evaluation of Automated Tools for Side-Channel Vulnerabilities Detection in Cryptographic Libraries**..... 1690  
Antoine Geimer (*Univ. Lille, CNRS, Inria, Univ. Rennes, CNRS, IRISA*),  
Mathéo Vergnolle (*Université Paris-Saclay, CEA, List*), Frédéric Recoules (*Université Paris-Saclay, CEA, List*),  
Lesly-Ann Daniel (*KU Leuven, imec-DistriNet*), Sébastien Bardin (*Université Paris-Saclay, CEA, List*),  
Clémentine Maurice (*Univ. Lille, CNRS, Inria*)
- **A Thorough Evaluation of RAMBAM**..... 1705  
Daniel Lammers (*Ruhr University Bochum*), Amir Moradi (*Ruhr University Bochum*),  
Nicolai Müller (*Ruhr University Bochum*), Aein Rezaei Shahmirzadi (*Ruhr University Bochum*)

## Session 30: Information Flow & Differential Privacy

- **A Novel Analysis of Utility in Privacy Pipelines, Using Kronecker Products and Quantitative Information Flow** ..... 1718  
Mário S. Alvim (*UFMG*), Natasha Fernandes (*Macquarie University*), Annabelle McIver (*Macquarie University*),  
Carroll Morgan (*UNSW & Trustworthy Systems*), Gabriel H. Nunes (*Macquarie University & UFMG*)
- **Tainted Secure Multi-Execution to Restrict Attacker Influence** ..... 1732  
McKenna McCall (*Carnegie Mellon University*),  
Abhishek Bichhawat (*Indian Institute of Technology Gandhinagar*), Limin Jia (*Carnegie Mellon University*)

- **Assume but Verify: Deductive Verification of Leaked Information in Concurrent Applications**..... 1746  
Toby Murray (*University of Melbourne*), Mukesh Tiwari (*University of Cambridge*),  
Gidon Ernst (*LMU Munich*), David A. Naumann (*Stevens Institute of Technology*)
- **Deciding Differential Privacy of Online Algorithms with Multiple Variables**..... 1761  
Rohit Chadha (*University of Missouri*), A. Prasad Sistla (*University of Illinois at Chicago*),  
Mahesh Viswanathan (*University of Illinois at Urbana-Champaign*), Bishnu Bhusal (*University of Missouri*)

## Session 31: Cryptography for Blockchains

- **FlexiRand: Output Private (Distributed) VRFs and Application to Blockchains**..... 1776  
Aniket Kate (*Purdue University & Supra Research*), Easwar Vivek Mangipudi (*Supra Research*),  
Siva Maradana (*Indian Statistical Institute*), Pratyay Mukherjee (*Supra Research*)
- **Adaptively Secure (Aggregatable) PVSS and Application to Distributed Randomness Beacons** ..... 1791  
Renas Bacho (*CISPA Helmholtz Center for Information Security & Universität des Saarlandes*),  
Julian Loss (*CISPA Helmholtz Center for Information Security*)
- **Short Privacy-Preserving Proofs of Liabilities**..... 1805  
Francesca Falzon (*Brown University, University of Chicago*), Kaoutar Elkhiyaoui (*IBM Research, Zürich*),  
Yacov Manevich (*IBM Research, Zürich*), Angelo De Caro (*IBM Research, Zürich*)
- **The Locality of Memory Checking**..... 1820  
Weijie Wang (*Yale University*), Yujie Lu (*Yale University*), Charalampos Papamanthou (*Yale University*),  
Fan Zhang (*Yale University*)

## Session 32: Language Models & Verification

- **Stealing the Decoding Algorithms of Language Models**..... 1835  
Ali Naseh (*University of Massachusetts Amherst*), Kalpesh Krishna (*University of Massachusetts Amherst*),  
Mohit Iyyer (*University of Massachusetts Amherst*), Amir Houmansadr (*University of Massachusetts Amherst*)
- **Verifiable Learning for Robust Tree Ensembles** ..... 1850  
Stefano Calzavara (*Università Ca' Foscari Venezia*), Lorenzo Cazzaro (*Università Ca' Foscari Venezia*),  
Giulio Ermanno Pibiri (*Università Ca' Foscari Venezia*), Nicola Prezza (*University Ca' Foscari Venezia*)
- **Large Language Models for Code: Security Hardening and Adversarial Testing**..... 1865  
Jingxuan He (*ETH Zurich*), Martin Vechev (*ETH Zurich*)
- **Experimenting with Zero-Knowledge Proofs of Training** ..... 1880  
Sanjam Garg (*University of California, Berkeley*), Aarushi Goel (*NTT Research*),  
Somesh Jha (*University of Wisconsin - Madison*), Saeed Mahloujifar (*Meta AI*),  
Mohammad Mahmoody (*University of Virginia*), Guru-Vamsi Policharla (*University of California, Berkeley*),  
Mingyuan Wang (*University of California, Berkeley*)

## Session 33: Differential Privacy

- **Group and Attack: Auditing Differential Privacy** ..... 1905  
Johan Lokna (*ETH Zurich*), Anouk Paradis (*ETH Zurich*), Dimitar I. Dimitrov (*ETH Zurich*),  
Martin Vechev (*ETH Zurich*)
- **Interactive Proofs For Differentially Private Counting** ..... 1919  
Ari Biswas (*University of Warwick*), Graham Cormode (*Meta AI*)
- **Concentrated Geo-Privacy** ..... 1934  
Yuting Liang (*Hong Kong University of Science and Technology*),  
Ke Yi (*Hong Kong University of Science and Technology*)
- **Concurrent Composition for Interactive Differential Privacy with Adaptive Privacy-Loss Parameters**..... 1949  
Samuel Haney (*Tumult Labs*), Michael Shoemate (*Harvard University*), Grace Tian (*Harvard University*),  
Salil Vadhan (*Harvard University*), Andrew Vyrros (*Harvard University*), Vicki Xu (*Harvard University*),  
Wanrong Zhang (*Harvard University*)

## Session 34: Kernel & System Calls

- **SysXCHG: Refining Privilege with Adaptive System Call Filters** ..... 1964  
Alexander J. Gaidis (*Brown University*), Vaggelis Atlidakis (*Brown University*),  
Vasileios P. Kemerlis (*Brown University*)

- **SysPART: Automated Temporal System Call Filtering for Binaries** ..... 1979  
Vidya Lakshmi Rajagopalan (*Stevens Institute of Technology*),  
Konstantinos Klefogiorgos (*Stevens Institute of Technology*), Enes Göktas (*Stevens Institute of Technology*),  
Jun Xu (*University of Utah*), Georgios Portokalidis (*Stevens Institute of Technology & IMDEA Software Institute*)
- **HACKSAW: Hardware-Centric Kernel Debloating via Device Inventory  
and Dependency Analysis** ..... 1994  
Zhenghao Hu (*New York University*), Sangho Lee (*Microsoft Research*), Marcus Peinado (*Microsoft Research*)
- **KROVER: A Symbolic Execution Engine for Dynamic Kernel Analysis** ..... 2009  
Pansilu Pitigalaarachchi (*Singapore Management University*), Xuhua Ding (*Singapore Management University*),  
Haiqing Qiu (*Singapore Management University*), Haoxin Tu (*Singapore Management University*),  
Jiaqi Hong (*Independent Researcher*), Lingxiao Jiang (*Singapore Management University*)

## Session 35: Speculative Execution & Information Flow

- **Gotcha! I Know What You Are Doing on the FPGA Cloud: Fingerprinting  
Co-Located Cloud FPGA Accelerators via Measuring Communication Links** ..... 2024  
Chongzhou Fang (*University of California, Davis*), Ning Miao (*University of California, Davis*),  
Han Wang (*Temple University*), Jiacheng Zhou (*University of California, Davis*),  
Tyler Sheaves (*University of California, Davis*), John M. Emmert (*University of Cincinnati*),  
Avesta Sasan (*University of California, Davis*), Houman Homayoun (*University of California, Davis*)
- **iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices** ..... 2038  
Jason Kim (*Georgia Tech*), Stephan van Schaik (*University of Michigan*), Daniel Genkin (*Georgia Tech*),  
Yuval Yarom (*Ruhr University Bochum*)
- **DECLASSIFLOW: A Static Analysis for Modeling Non-Speculative Knowledge  
to Relax Speculative Execution Security Measures** ..... 2053  
Rutvik Choudhary (*University of Illinois Urbana Champaign*),  
Alan Wang (*University of Illinois Urbana Champaign*),  
Zirui Neil Zhao (*University of Illinois Urbana Champaign*), Adam Morrison (*Tel Aviv University*),  
Christopher W. Fletcher (*University of Illinois Urbana Champaign*)
- **SpecVerilog: Adapting Information Flow Control for Secure Speculation** ..... 2068  
Drew Zagieboylo (*Cornell University*), Charles Sherk (*Cornell University*), Andrew C. Myers (*Cornell University*),  
G. Edward Suh (*Cornell University*)

## Session 36: Verified Cryptographic Implementations

- **Formalizing, Verifying and Applying ISA Security Guarantees as Universal Contracts**..... 2083  
Sander Huyghebaert (*Vrije Universiteit Brussel & KU Leuven*), Steven Keuchel (*Vrije Universiteit Brussel*),  
Coen De Roover (*Vrije Universiteit Brussel*), Dominique Devriese (*KU Leuven*)
- **Boosting the Performance of High-Assurance Cryptography: Parallel Execution  
and Optimizing Memory Access in Formally-Verified Line-Point Zero-Knowledge** ..... 2098  
Samuel Dittmer (*Stealth Software Technologies, Inc.*), Karim Eldefrawy (*SRI International*),  
Stéphane Graham-Lengrand (*SRI International*), Steve Lu (*Stealth Software Technologies, Inc.*),  
Rafail Ostrovsky (*University of California, Los Angeles*), Vitor Pereira (*SRI International*)
- **Galápagos: Developing Verified Low Level Cryptography on Heterogeneous Hardware** ... 2113  
Yi Zhou (*Carnegie Mellon University*), Sydney Gibson (*Carnegie Mellon University*), Sarah Cai (*Databricks*),  
Menucha Winchell (*University of California, Berkeley*), Bryan Parno (*Carnegie Mellon University*)
- **Specification and Verification of Side-channel Security for Open-source Processors  
via Leakage Contracts** ..... 2128  
Zilong Wang (*IMDEA Software Institute & Universidad Politécnica de Madrid*),  
Gideon Mohr (*Saarland University*), Klaus von Gleissenthall (*Vrije Universiteit Amsterdam*),  
Jan Reineke (*Saarland University*), Marco Guarnieri (*IMDEA Software Institute*)

## Session 37: Multiparty Computation I

- **GROTTO: Screaming fast (2+1)-PC or  $\mathbb{Z}_2^n$  via (2,2)-DPFs** ..... 2143  
Kyle Storrer (*University of Calgary*), Adithya Vadapalli (*IIT Kanpur*),  
Allan Lyons (*University of Calgary*), Ryan Henry (*University of Calgary*)
- **Scalable Multiparty Garbling** ..... 2158  
Gabrielle Beck (*Johns Hopkins University*), Aarushi Goel (*NTT Research*),  
Aditya Hegde (*Johns Hopkins University*), Abhishek Jain (*Johns Hopkins University & NTT Research*),  
Zhengzhong Jin (*Massachusetts Institute of Technology*), Gabriel Kaptchuk (*Boston University*)



- **Linear Communication in Malicious Majority MPC** ..... 2173  
S. Dov Gordon (*George Mason University & TripleBlind*),  
Phi Hung Le (*George Mason University*), Daniel McVicker (*George Mason University*)
- **Efficient Multiparty Probabilistic Threshold Private Set Intersection** ..... 2188  
Feng-Hao Liu (*Washington State University*), En Zhang (*Henan Normal University*),  
Leiyong Qin (*Henan Normal University*)

## Session 38: Network Security

- **Vulnerability Intelligence Alignment via Masked Graph Attention Networks** ..... 2202  
Yue Qin (*Indiana University Bloomington*), Yue Xiao (*Indiana University Bloomington*),  
Xiaojing Liao (*Indiana University Bloomington*)
- **In Search of netUnicorn: A Data-Collection Platform to Develop Generalizable ML Models for Network Security Problems**..... 2217  
Roman Beltiukov (*UC Santa Barbara*), Wenbo Guo (*Purdue University*),  
Arpit Gupta (*UC Santa Barbara*), Walter Willinger (*NIKSUN, Inc.*)
- **MDTD: A Multi-Domain Trojan Detector for Deep Neural Networks** ..... 2232  
Arezoo Rajabi (*University of Washington*), Surudhi Asokraj (*University of Washington*),  
Fengqing Jiang (*University of Washington*), Luyao Niu (*University of Washington*),  
Bhaskar Ramasubramanian (*Western Washington University*), James Ritcey (*University of Washington*),  
Radha Poovendran (*University of Washington*)
- **PROVG-SEARCHER: A Graph Representation Learning Approach for Efficient Provenance Graph Search** ..... 2247  
Enes Altinisik (*Qatar Computing Research Institute, HBKU*),  
Fatih Deniz (*Qatar Computing Research Institute, HBKU*),  
Hüsrev Taha Sencar (*Qatar Computing Research Institute, HBKU*)

## Session 39: Privacy in Computation

- **Securely Sampling Discrete Gaussian Noise for Multi-Party Differential Privacy** ..... 2262  
Chengkun Wei (*Zhejiang University*), Ruijing Yu (*Zhejiang University*), Yuan Fan (*Zhejiang University*),  
Wenzhi Chen (*Zhejiang University*), Tianhao Wang (*University of Virginia*)
- **Detecting Violations of Differential Privacy for Quantum Algorithms** ..... 2277  
Ji Guan (*State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences*),  
Wang Fang (*State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences*),  
Mingyu Huang (*State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences*),  
Mingsheng Ying (*State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences & Tsinghua University*)
- **Amplification by Shuffling without Shuffling** ..... 2292  
Borja Balle (*Google Deepmind*), James Bell (*Google*), Adrià Gascón (*Google*)
- **HELiKs: HE Linear Algebra Kernels for Secure Inference** ..... 2306  
Shashank Balla (*University of California San Diego*), Farinaz Koushanfar (*University of California San Diego*)

## Session 40: Medley

- **SkillScanner: Detecting Policy-Violating Voice Applications Through Static Analysis at the Development Phase** ..... 2321  
Song Liao (*Clemson University*), Long Cheng (*Clemson University*), Haipeng Cai (*Washington State University*),  
Linke Guo (*Clemson University*), Hongxin Hu (*University at Buffalo*)
- **Protecting Intellectual Property of Large Language Model-Based Code Generation APIs via Watermarks**..... 2336  
Zongjie Li (*Hong Kong University of Science and Technology*), Chaozheng Wang (*Harbin Institute of Technology*),  
Shuai Wang (*Hong Kong University of Science and Technology*), Cuiyun Gao (*Harbin Institute of Technology*)
- **Simplifying Mixed Boolean-Arithmetic Obfuscation by Program Synthesis and Term Rewriting**..... 2351  
Jaehyung Lee (*Hanyang University*), Woosuk Lee (*Hanyang University*)

- **Enhancing OSS Patch Backporting with Semantics**..... 2366  
 Su Yang (*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*),  
 Yang Xiao (*Institute of Information Engineering, Chinese Academy of Sciences & University of Chinese Academy of Sciences*),  
 Zhengzi Xu (*Nanyang Technological University*),  
 Chengyi Sun (*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences*),  
 Chen Ji (*Xidian University*),  
 Yuqing Zhang (*University of Chinese Academy of Sciences, Xidian University, & Hainan University*)

## Session 41: Measuring Security Deployments

- **Evaluating the Security Posture of Real-World FIDO2 Deployments**..... 2381  
 Dhruv Kuchhal (*Georgia Institute of Technology*), Muhammad Saad (*PayPal, Inc.*),  
 Adam Oest (*PayPal, Inc.*), Frank Li (*Georgia Institute of Technology*)
- **Are we there yet? An Industrial Viewpoint on Provenance-based Endpoint Detection and Response Tools**..... 2396  
 Feng Dong (*Huazhong University of Science and Technology*), Shaofei Li (*Peking University*),  
 Peng Jiang (*Peking University*), Ding Li (*Peking University*),  
 Haoyu Wang (*Huazhong University of Science and Technology*), Liangyi Huang (*Arizona State University*),  
 Xusheng Xiao (*Arizona State University*), Jiedong Chen (*Sangfor Technologies Inc.*),  
 Xiapu Luo (*The Hong Kong Polytechnic University*), Yao Guo (*Peking University*),  
 Xiangqun Chen (*Peking University*)
- **Don't Leak Your Keys: Understanding, Measuring, and Exploiting the AppSecret Leaks in Mini-Programs** ..... 2411  
 Yue Zhang (*The Ohio State University*), Yuqing Yang (*The Ohio State University*),  
 Zhiqiang Lin (*The Ohio State University*)
- **The Effectiveness of Security Interventions on GitHub** ..... 2426  
 Felix Fischer (*Technical University of Munich*), Jonas Höbenreich (*Technical University of Munich*),  
 Jens Grossklags (*Technical University of Munich*)

## Session 42: Attacking the Web

- **CoCo: Efficient Browser Extension Vulnerability Detection via Coverage-guided, Concurrent Abstract Interpretation** ..... 2441  
 Jianjia Yu (*Johns Hopkins University*), Song Li (*Zhejiang University*),  
 Junmin Zhu (*Shanghai Jiao Tong University*), Yinzhi Cao (*Johns Hopkins University*)
- **Finding All Cross-Site Needles in the DOM Stack: A Comprehensive Methodology for the Automatic XS-Leak Detection in Web Browsers** ..... 2456  
 Dominik Trevor Noß (*Ruhr University Bochum*), Lukas Knittel (*Ruhr University Bochum*),  
 Christian Mainka (*Ruhr University Bochum*), Marcus Niemietz (*Niederrhein University of Applied Sciences*),  
 Jörg Schwenk (*Ruhr University Bochum*)
- **Uncovering and Exploiting Hidden APIs in Mobile Super Apps** ..... 2471  
 Chao Wang (*The Ohio State University*), Yue Zhang (*The Ohio State University*),  
 Zhiqiang Lin (*The Ohio State University*)
- **A Good Fishman Knows All the Angles: A Critical Evaluation of Google's Phishing Page Classifier** ..... 2486  
 Changqing Miao (*Renmin University of China*), Jianan Feng (*Renmin University of China*),  
 Wei You (*Renmin University of China*), Wenchang Shi (*Renmin University of China*),  
 Jianjun Huang (*Renmin University of China*), Bin Liang (*Renmin University of China*)

## Session 43: Multiparty Computation II

- **Improved Distributed RSA Key Generation Using the Miller-Rabin Test** ..... 2501  
 Jakob Burkhardt (*Aarhus University*), Ivan Damgård (*Aarhus University*), Tore Kasper Frederiksen (*Zama*),  
 Satrajit Ghosh (*Indian Institute of Technology Kharagpur*), Claudio Orlandi (*Aarhus University*)
- **Towards Generic MPC Compilers via Variable Instruction Set Architectures (VISAs)** ..... 2516  
 Yibin Yang (*Georgia Institute of Technology*), Stanislav Peceny (*Georgia Institute of Technology*),  
 David Heath (*University of Illinois Urbana-Champaign*), Vladimir Kolesnikov (*Georgia Institute of Technology*)

- **COMBINE: COMpilation and Backend-INdependent vEctorization for Multi-Party Computation** ..... 2531  
Benjamin Levy (*Rensselaer Polytechnic Institute (RPI)*), Muhammad Ishaq (*Purdue University*), Benjamin Sherman (*Rensselaer Polytechnic Institute (RPI)*), Lindsey Kennard (*Rensselaer Polytechnic Institute (RPI)*), Ana Milanova (*Rensselaer Polytechnic Institute (RPI)*), Vassilis Zikas (*Purdue University*)
- **Let's Go Eevee! A Friendly and Suitable Family of AEAD Modes for IoT-to-Cloud Secure Computation** ..... 2546  
Amit Singh Bhati (*KU Leuven*), Erik Pohle (*KU Leuven*), Aysajan Abidin (*KU Leuven*), Elena Andreeva (*Technical University of Vienna*), Bart Preneel (*KU Leuven*)

## Session 44: Machine Learning, Cryptography, & Cyber-Physical Systems

- **On the Security of KZG Commitment for VSS** ..... 2561  
Atsuki Momose (*University of Illinois at Urbana-Champaign*), Sourav Das (*University of Illinois at Urbana-Champaign*), Ling Ren (*University of Illinois at Urbana-Champaign*)
- **Targeted Attack Synthesis for Smart Grid Vulnerability Analysis** ..... 2576  
Suman Maiti (*Indian Institute of Technology Kharagpur*), Anjana Balabhaskara (*Indian Institute of Technology Kharagpur*), Sunandan Adhikary (*Indian Institute of Technology Kharagpur*), Ipsita Koley (*Indian Institute of Technology Kharagpur*), Soumyajit Dey (*Indian Institute of Technology Kharagpur*)
- **Secure and Timely GPU Execution in Cyber-physical Systems** ..... 2591  
Jinwen Wang (*Washington University in St. Louis*), Yujie Wang (*Washington University in St. Louis*), Ning Zhang (*Washington University in St. Louis*)
- **SALSA PICANTE: A Machine Learning Attack on LWE with Binary Secrets** ..... 2606  
Cathy Yuanchen Li (*Meta AI*), Jana Sotáková (*Meta AI*), Emily Wenger (*The University of Chicago*), Mohamed Malhou (*Meta AI*), Evrard Garcelon (*Meta AI*), François Charton (*Meta AI*), Kristin Lauter (*Meta AI*)

## Session 45: Privacy in Machine Learning

- **DPMLBench: Holistic Evaluation of Differentially Private Machine Learning** ..... 2621  
Chengkun Wei (*Zhejiang University*), Minghu Zhao (*Zhejiang University*), Zhikun Zhang (*Stanford University & CISA Helmholtz Center for Information Security*), Min Chen (*CISA Helmholtz Center for Information Security*), Wenlong Meng (*Zhejiang University*), Bo Liu (*Dbappsecurity*), Yuan Fan (*Zhejiang University*), Wenzhi Chen (*Zhejiang University*)
- **Geometry of Sensitivity: Twice Sampling and Hybrid Clipping in Differential Privacy with Optimal Gaussian Noise and Application to Deep Learning** ..... 2636  
Hanshen Xiao (*Massachusetts Institute of Technology*), Jun Wan (*Massachusetts Institute of Technology*), Srinivas Devadas (*Massachusetts Institute of Technology*)
- **Blink: Link Local Differential Privacy in Graph Neural Networks via Bayesian Estimation** ..... 2651  
Xiaochen Zhu (*National University of Singapore*), Vincent Y. F. Tan (*National University of Singapore*), Xiaokui Xiao (*National University of Singapore*)
- **DP-Forward: Fine-tuning and Inference on Language Models with Differential Privacy in Forward Pass** ..... 2665  
Minxin Du (*The Chinese University of Hong Kong*), Xiang Yue (*The Ohio State University*), Sherman S. M. Chow (*The Chinese University of Hong Kong*), Tianhao Wang (*University of Virginia*), Chenyu Huang (*Independent Researcher*), Huan Sun (*The Ohio State University*)

## Session 46: Program Analysis & Instrumentation

- **Whole-Program Control-Flow Path Attestation** ..... 2680  
Nikita Yadav (*Indian Institute of Science*), Vinod Ganapathy (*Indian Institute of Science*)
- **Improving Security Tasks Using Compiler Provenance Information Recovered At the Binary-Level** ..... 2695  
Yufei Du (*Georgia Institute of Technology*), Omar Alrawi (*Georgia Institute of Technology*), Kevin Snow (*Zeropoint Dynamics*), Manos Antonakakis (*Georgia Institute of Technology*), Fabian Monrose (*Georgia Institute of Technology*)

- **SYMGX: Detecting Cross-boundary Pointer Vulnerabilities of SGX Applications via Static Symbolic Execution** ..... 2710  
Yuanpeng Wang (*Peking University*), Ziqi Zhang (*Peking University*), Ningyu He (*Peking University*),  
Zhineng Zhong (*Peking University*), Shengjian Guo (*Independent Researcher*),  
Qinkun Bao (*Independent Researcher*), Ding Li (*Peking University*), Yao Guo (*Peking University*),  
Xiangqun Chen (*Peking University*)
- **TYPESQUEEZER: When Static Recovery of Function Signatures for Binary Executables Meets Dynamic Analysis**..... 2725  
Ziyi Lin (*Xidian University*), Jinku Li (*Xidian University*), Bowen Li (*Xidian University*),  
Haoyu Ma (*Zhejiang Lab*), Debin Gao (*Singapore Management University*), Jianfeng Ma (*Xidian University*)

## Session 47: Security Professionals

- **“Make Them Change it Every Week!”: A Qualitative Exploration of Online Developer Advice on Usable and Secure Authentication** ..... 2740  
Jan H. Klemmer (*Leibniz University Hannover*), Marco Gutfleisch (*Ruhr University Bochum*),  
Christian Stransky (*CISPA Helmholtz Center for Information Security*), Yasemin Acar (*Paderborn University*),  
M. Angela Sasse (*Ruhr University Bochum*), Sascha Fahl (*CISPA Helmholtz Center for Information Security*)
- **Sharing Communities: The Good, the Bad, and the Ugly**..... 2755  
Thomas Geras (*HM Munich University of Applied Sciences*),  
Thomas Schreck (*HM Munich University of Applied Sciences*)
- **Alert Alchemy: SOC Workflows and Decisions in the Management of NIDS Rules** ..... 2770  
Mathew Vermeer (*Delft University of Technology*), Natalia Kadenko (*Delft University of Technology*),  
Michel van Eeten (*Delft University of Technology*), Carlos Gañán (*Delft University of Technology*),  
Simon Parkin (*Delft University of Technology*)
- **Do Users Write More Insecure Code with AI Assistants?**..... 2785  
Neil Perry (*Stanford University*), Megha Srivastava (*Stanford University*),  
Deepak Kumar (*Stanford University & UC San Diego*), Dan Boneh (*Stanford University*)

## Session 48: Defending the Web

- **HODOR: Shrinking Attack Surface on Node.js via System Call Limitation** ..... 2800  
Wenya Wang (*Shanghai Jiao Tong University*), Xingwei Lin (*Ant Group*),  
Jingyi Wang (*Zhejiang University & ZJU-Hangzhou Global Scientific and Technological Innovation Center*),  
Wang Gao (*Shanghai Jiao Tong University*), Dawu Gu (*Shanghai Jiao Tong University*), Wei Lv (*Ant Group*),  
Jiashui Wang (*Zhejiang University & Ant Group*)
- **ADEM: An Authentic Digital Emblem** ..... 2815  
Felix Linker (*ETH Zurich*), David Basin (*ETH Zurich*)
- **Is Modeling Access Control Worth It?** ..... 2830  
David Basin (*ETH Zürich*), Juan Guarnizo (*ETH Zürich*), Srđan Krstić (*ETH Zürich*),  
Hoang Nguyen (*ETH Zürich*), Martín Ochoa (*Zurich University of Applied Sciences*)
- **Fine-Grained Data-Centric Content Protection Policy for Web Applications** ..... 2845  
Zilun Wang (*The Chinese University of Hong Kong*), Wei Meng (*The Chinese University of Hong Kong*),  
Michael R. Lyu (*The Chinese University of Hong Kong*)

## Session 49: Cryptographic Protocols

- **On the Security of Rate-limited Privacy Pass** ..... 2871  
Hien Chu (*Friedrich Alexander Universität Erlangen-Nürnberg*),  
Khue Do (*CISPA Helmholtz Center for Information Security*),  
Lucjan Hanzlik (*CISPA Helmholtz Center for Information Security*)
- **Passive SSH Key Compromise via Lattices**..... 2886  
Keegan Ryan (*University of California, San Diego*),  
Kaiwen He (*University of California, San Diego & Massachusetts Institute of Technology*),  
George Arnold Sullivan (*University of California, San Diego*),  
Nadia Heninger (*University of California, San Diego*)
- **Stealth Key Exchange and Confined Access to the Record Protocol Data in TLS 1.3** ..... 2901  
Marc Fischlin (*Technische Universität Darmstadt*)

- **ELEKTRA: Efficient Lightweight multi-dEvice Key TRAnsparency** ..... 2915  
Julia Len (*Cornell Tech*), Melissa Chase (*Microsoft Research*), Esha Ghosh (*Microsoft Research*),  
Daniel Jost (*New York University*), Balachandar Kesavan (*Zoom Video Communications*),  
Antonio Marcedone (*Zoom Video Communications*)

## Session 50: Homomorphic Encryption II

- **HE<sup>3</sup>DB: An Efficient and Elastic Encrypted Database Via Arithmetic-And-Logic Fully Homomorphic Encryption** ..... 2930  
Song Bian (*Beihang University*), Zhou Zhang (*Beihang University*), Haowen Pan (*Beihang University*),  
Ran Mao (*Beihang University*), Zian Zhao (*Beihang University*),  
Yier Jin (*University of Science and Technology of China*), Zhenyu Guan (*Beihang University*)
- **Level Up: Private Non-Interactive Decision Tree Evaluation using Levelled Homomorphic Encryption** ..... 2945  
Rasoul Akhavan Mahdavi (*University of Waterloo*), Haoyan Ni (*University of Waterloo*),  
Dimitry Linkov (*University of Waterloo*), Florian Kerschbaum (*University of Waterloo*)
- **Fast Unbalanced Private Set Union from Fully Homomorphic Encryption** ..... 2959  
Binbin Tu (*Shandong University*), Yu Chen (*Shandong University*), Qi Liu (*Shandong University*),  
Cong Zhang (*IIIE, CAS*)
- **Efficient Multiplicative-to-Additive Function from Joye-Libert Cryptosystem and Its Application to Threshold ECDSA** ..... 2974  
Haiyang Xue (*The Hong Kong Polytechnic University*), Man Ho Au (*The Hong Kong Polytechnic University*),  
Mengling Liu (*The Hong Kong Polytechnic University*), Kwan Yin Chan (*The University of Hong Kong*),  
Handong Cui (*The University of Hong Kong*), Xiang Xie (*Shanghai Qizhi Institute, PADO Labs*),  
Tsz Hon Yuen (*The University of Hong Kong*), Chengru Zhang (*The University of Hong Kong*)

## Session 51: Privacy in Systems

- **SPLICE: Efficiently Removing a User's Data from In-memory Application State** ..... 2989  
Xueyuan Han (*Wake Forest University*), James Mickens (*Harvard University*),  
Siddhartha Sen (*Microsoft Research*)
- **Leakage-Abuse Attacks Against Forward and Backward Private Searchable Symmetric Encryption** ..... 3003  
Lei Xu (*Nanjing University of Science and Technology & City Univeristy of Hong Kong*),  
Leqian Zheng (*City Univeristy of Hong Kong*), Chengzhi Xu (*Nanjing University of Science and Technology*),  
Xingliang Yuan (*Monash University*), Cong Wang (*City University of Hong Kong*)
- **Using Range-Revocable Pseudonyms to Provide Backward Unlinkability in the Edge**..... 3018  
Cláudio Correia (*INESC-ID, Instituto Superior Técnico, Universidade de Lisboa*),  
Miguel Correia (*INESC-ID, Instituto Superior Técnico, Universidade de Lisboa*),  
Luís Rodrigues (*INESC-ID, Instituto Superior Técnico, Universidade de Lisboa*)
- **Shufflecake: Plausible Deniability for Multiple Hidden Filesystems on Linux**..... 3033  
Elia Anzuoni (*Kudelski Security & École Polytechnique Fédérale de Lausanne*),  
Tommaso Gagliardoni (*Kudelski Security*)

## Session 52: Attacks & Malware

- **Take Over the Whole Cluster: Attacking Kubernetes via Excessive Permissions of Third-party Applications** ..... 3048  
Nanzi Yang (*Xidian University*), Wenbo Shen (*Zhejiang University*), Jinku Li (*Xidian University*),  
Xunqi Liu (*Xidian University*), Xin Guo (*Xidian University*), Jianfeng Ma (*Xidian University*)
- **Lost along the Way: Understanding and Mitigating Path-Misresolution Threats to Container Isolation** ..... 3063  
Zhi Li (*Huazhong University of Science and Technology*), Weijie Liu (*Ant Group*),  
XiaoFeng Wang (*Indiana University Bloomington*), Bin Yuan (*Huazhong University of Science and Technology*),  
Hongliang Tian (*Ant Group*), Hai Jin (*Huazhong University of Science and Technology*),  
Shoumeng Yan (*Ant Group*)

- **PackGenome: Automatically Generating Robust YARA Rules for Accurate Malware Packer Detection** ..... 3078  
Shijia Li (*Nankai University, TKLNDST, & DISSEC*), Jiang Ming (*Tulane University*), Pengda Qiu (*Nankai University, TKLNDST, & DISSEC*), Qiyuan Chen (*Nankai University, TKLNDST, & DISSEC*), Lanqing Liu (*Nankai University, TKLNDST, & DISSEC*), Huaifeng Bao (*SKLOIS, IIE*), Qiang Wang (*SKLOIS, IIE*), Chunfu Jia (*Nankai University, TKLNDST, & DISSEC*)
- **RetSpill: Igniting User-Controlled Data to Burn Away Linux Kernel Protections** ..... 3093  
Kyle Zeng (*Arizona State University*), Zhenpeng Lin (*Northwestern University*), Kangjie Lu (*University of Minnesota*), Xinyu Xing (*Northwestern University*), Ruoyu Wang (*Arizona State University*), Adam Doupe (*Arizona State University*), Yan Shoshitaishvili (*Arizona State University*), Tiffany Bao (*Arizona State University*)

## Session 53: Usable Authentication

- **Measuring Website Password Creation Policies At Scale** ..... 3108  
Suood Alroomi (*Georgia Institute of Technology*), Frank Li (*Georgia Institute of Technology*)
- **“I just stopped using one and started using the other”: Motivations, Techniques, and Challenges When Switching Password Managers** ..... 3123  
Collins W. Munyendo (*The George Washington University*), Peter Mayer (*University of Southern Denmark*), Adam J. Aviv (*The George Washington University*)
- **“We’ve Disabled MFA for You”: An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments** ..... 3138  
Sabrina Klivan (*CISPA Helmholtz Center for Information Security*), Sandra Höltervennhoff (*Leibniz University Hannover*), Nicolas Huaman (*Leibniz University Hannover*), Alexander Krause (*CISPA Helmholtz Center for Information Security*), Lucy Simko (*The George Washington University*), Yasemin Acar (*Paderborn University & The George Washington University*), Sascha Fahl (*CISPA Helmholtz Center for Information Security*)
- **Uncovering Impact of Mental Models towards Adoption of Multi-device Crypto-Wallets ...** 3153  
Easwar Vivek Mangipudi (*Supra Research*), Udit Desai (*IIT Kharagpur*), Mohsen Minaei (*Visa Research*), Mainack Mondal (*IIT Kharagpur*), Aniket Kate (*Purdue University & Supra Research*)

## Session 54: Measuring the Web

- **You Call This Archaeology? Evaluating Web Archives for Reproducible Web Security Measurements** ..... 3168  
Florian Hantke (*CISPA Helmholtz Center for Information Security*), Stefano Calzavara (*Università Ca’ Foscari Venezia*), Moritz Wilhelm (*CISPA Helmholtz Center for Information Security*), Alvise Rabitti (*Università Ca’ Foscari Venezia*), Ben Stock (*CISPA Helmholtz Center for Information Security*)
- **Cybercrime Bitcoin Revenue Estimations: Quantifying the Impact of Methodology and Coverage** ..... 3183  
Gibran Gomez (*IMDEA Software Institute & Universidad Politécnica de Madrid*), Kevin van Liebergen (*IMDEA Software Institute & Universidad Politécnica de Madrid*), Juan Caballero (*IMDEA Software Institute*)
- **Jack-in-the-box: An Empirical Study of JavaScript Bundling on the Web and its Security Implications** ..... 3198  
Jeremy Rack (*CISPA Helmholtz Center for Information Security*), Cristian-Alexandru Staicu (*CISPA Helmholtz Center for Information Security*)
- **Understanding and Detecting Abused Image Hosting Modules as Malicious Services** ..... 3213  
Geng Hong (*Fudan University*), Mengying Wu (*Fudan University*), Pei Chen (*Fudan University*), Xiaojing Liao (*Indiana University Bloomington*), Guoyi Ye (*Fudan University*), Min Yang (*Fudan University*)

## Session 55: Security of Cryptographic Protocols & Implementations

- **Faster Constant-time Evaluation of the Kronecker Symbol with Application to Elliptic Curve Hashing** ..... 3228  
Diego F. Aranha (*Aarhus University*), Benjamin Salling Hvass (*Aarhus University*), Bas Spitters (*Aarhus University*), Mehdi Tibouchi (*NTT Corporation*)

- **Verifiable Verification in Cryptographic Protocols**..... 3239  
Marc Fischlin (*Technische Universität Darmstadt*), Felix Günther (*ETH Zürich & IBM Research Europe - Zurich*)
- **Compact Frequency Estimators in Adversarial Environments** ..... 3254  
Sam A. Markelon (*University of Florida*), Mia Filić (*ETH Zürich*), Thomas Shrimpton (*University of Florida*)
- **ACABELLA: Automated (Crypt)analysis of Attribute-Based Encryption Leveraging Linear Algebra** ..... 3269  
Antonio de la Piedra (*Kudelski Security Research Team*),  
Marloes Venema (*Radboud University & University of Wuppertal*),  
Greg Alpar (*Open University of the Netherlands & Radboud University*)

## Session 56: Oblivious Algorithms & Data Structures

- **Ramen: Souper Fast Three-Party Computation for RAM Programs**..... 3284  
Lennart Braun (*Aarhus University*), Mahak Pancholi (*Aarhus University*), Rahul Rachuri (*Visa Research*),  
Mark Simkin (*Ethereum Foundation*)
- **Secure Statistical Analysis on Multiple Datasets: Join and Group-By** ..... 3298  
Gilad Asharov (*Bar-Ilan University*), Koki Hamada (*NTT Corporation*), Ryo Kikuchi (*NTT Corporation*),  
Ariel Nof (*Bar-Ilan University*), Benny Pinkas (*Bar-Ilan University & Aptos Labs*),  
Junichi Tomida (*NTT Corporation*)
- **FutORAMA: A Concretely Efficient Hierarchical Oblivious RAM**..... 3313  
Gilad Asharov (*Bar-Ilan University*), Ilan Komargodski (*Hebrew University & NTT Research*),  
Yehuda Michelson (*Bar-Ilan University*)
- **Waks-On/Waks-Off: Fast Oblivious Offline/Online Shuffling and Sorting with Waksman Networks** ..... 3328  
Sajin Sasy (*University of Waterloo*), Aaron Johnson (*U.S. Naval Research Laboratory*),  
Ian Goldberg (*University of Waterloo*)

## Session 57: Privacy in the Digital World

- **General Data Protection Runtime: Enforcing Transparent GDPR Compliance for Existing Applications** ..... 3343  
David Klein (*Technische Universität Braunschweig*), Benny Rolle (*SAP SE*),  
Thomas Barber (*SAP Security Research*), Manuel Karl (*Technische Universität Braunschweig*),  
Martin Johns (*Technische Universität Braunschweig*)
- **Control, Confidentiality, and the Right to be Forgotten** ..... 3358  
Aloni Cohen (*University of Chicago*), Adam Smith (*Boston University*),  
Marika Swanberg (*Boston University*), Prashant Nalini Vasudevan (*National University of Singapore*)
- **PolicyChecker: Analyzing the GDPR Completeness of Mobile Apps' Privacy Policies** ..... 3373  
Anhao Xiang (*Colorado School of Mines*), Weiping Pei (*The University of Tulsa*),  
Chuan Yue (*Colorado School of Mines*)
- **Speranza: Usable, Privacy-friendly Software Signing**..... 3388  
Kelsey Merrill (*MIT*), Zachary Newman (*Chainguard, Inc.*), Santiago Torres-Arias (*Purdue University*),  
Karen R. Sollins (*MIT*)

## Session 58: Measuring Machine Learning & Software Security

- **Unsafe Diffusion: On the Generation of Unsafe Images and Hateful Memes From Text-To-Image Models** ..... 3403  
Yiting Qu (*CISPA Helmholtz Center for Information Security*),  
Xinyue Shen (*CISPA Helmholtz Center for Information Security*),  
Xinlei He (*CISPA Helmholtz Center for Information Security*),  
Michael Backes (*CISPA Helmholtz Center for Information Security*),  
Savvas Zannettou (*Delft University of Technology*),  
Yang Zhang (*CISPA Helmholtz Center for Information Security*)
- **DE-FAKE: Detection and Attribution of Fake Images Generated by Text-to-Image Generation Models**..... 3418  
Zeyang Sha (*CISPA Helmholtz Center for Information Security*),  
Zheng Li (*CISPA Helmholtz Center for Information Security*), Ning Yu (*Salesforce Research*),  
Yang Zhang (*CISPA Helmholtz Center for Information Security*)

- **“Get in Researchers; We’re Measuring Reproducibility”: A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences**..... 3433  
Daniel Olszewski (*University of Florida*), Allison Lu (*University of Florida*),  
Carson Stillman (*University of Florida*), Kevin Warren (*University of Florida*),  
Cole Kitroser (*University of Florida*), Alejandro Pascual (*University of Florida*),  
Divyajyoti Ukirde (*University of Florida*), Kevin Butler (*University of Florida*),  
Patrick Traynor (*University of Florida*)
- **Unhelpful Assumptions in Software Security Research** ..... 3460  
Ita Ryan (*University College Cork*), Utz Roedig (*University College Cork*), Klaas-Jan Stol (*University College Cork*)

## Session 59: Tracking the Web

- **Read Between the Lines: Detecting Tracking JavaScript with Bytecode Classification**..... 3475  
Mohammad Ghasemisharif (*University of Illinois Chicago*), Jason Polakis (*University of Illinois Chicago*)
- **COOKIEGRAPH: Understanding and Detecting First-Party Tracking Cookies**..... 3490  
Shaoor Munir (*University of California, Davis*), Sandra Siby (*Imperial College London*),  
Umar Iqbal (*Washington University in St. Louis*), Steven Englehardt (*Independent Researcher*),  
Zubair Shafiq (*University of California, Davis*), Carmela Troncoso (*EPFL*)
- **ADCPG: Classifying JavaScript Code Property Graphs with Explanations for Ad and Tracker Blocking** ..... 3505  
Changmin Lee (*KAIST*), Soeul Son (*KAIST*)

## Session 60: Poster Session

- **Poster: Using CodeQL to Detect Malware in npm** ..... 3519  
Matias F. Gobbi (*Bundeswehr University Munich*),  
Johannes Kinder (*Ludwig-Maximilians-Universität München (LMU Munich)*)
- **Poster: Data Minimization by Construction for Trigger-Action Applications** ..... 3522  
Mohammad M. Ahmadpanah (*Chalmers University of Technology*),  
Daniel Hedin (*Chalmers University of Technology & Mälardalen University*),  
Andrei Sabelfeld (*Chalmers University of Technology*)
- **Poster: Verifiable Encodings for Maliciously-Secure Homomorphic Encryption Evaluation ...** 3525  
Sylvain Chatel (*EPFL*), Christian Knabenhans (*EPFL*), Apostolos Pyrgelis (*EPFL*),  
Carmela Troncoso (*EPFL*), Jean-Pierre Hubaux (*EPFL*)
- **Poster: Circumventing the GFW with TLS Record Fragmentation** ..... 3528  
Niklas Niere (*Paderborn University*), Sven Hebrok (*Paderborn University*),  
Juraj Somorovsky (*Paderborn University*), Robert Merget (*Technology Innovation Institute*)
- **Poster: Generating Experiences for Autonomous Network Defense** ..... 3531  
Andres Molina-Markham (*The MITRE Corporation*), Luis F. Robaina (*The MITRE Corporation*),  
Akash H. Trivedi (*The MITRE Corporation*), Derek G. Tsui (*The MITRE Corporation*), Ahmad Ridley (*NSA*)
- **Poster: From Hashes to Ashes – A Comparison of Transcription Services**..... 3534  
Rudolf Siegel (*CISPA Helmholtz Center for Information Security*),  
Rafael Mrowczynski (*CISPA Helmholtz Center for Information Security*),  
Maria Hellenthal (*CISPA Helmholtz Center for Information Security*),  
Michael Schilling (*CISPA Helmholtz Center for Information Security*)
- **Poster: *Mujaz*: A Summarization-based Approach for Normalized Vulnerability Description** ..... 3537  
Hattan Althebeiti (*University of Central Florida*), Brett Fazio (*Two Sigma*),  
William Chen (*Carnegie Mellon University*), David Mohaisen (*University of Central Florida*)
- **Poster: Boosting Adversarial Robustness by Adversarial Pre-training** ..... 3540  
Xiaoyun Xu (*Radboud University*), Stjepan Picek (*Radboud University*)
- **Poster: VULCAN -- Repurposing Accessibility Features for Behavior-based Intrusion Detection Dataset Generation**..... 3543  
Christian van Sloun (*RWTH Aachen University*), Klaus Wehrle (*RWTH Aachen University*)
- **Poster: Computing the Persistent Homology of Encrypted Data**..... 3546  
Dominic Gold (*Florida Atlantic University*),  
Koray Karabina (*National Research Council Canada & University of Waterloo*),  
Francis Motta (*Florida Atlantic University*)



- **Poster: Attestor -- Simple Proof-of-Storage-Time** ..... 3549  
Arup Mondal (*Ashoka University*)
- **Poster: Query-efficient Black-box Attack for Image Forgery Localization via Reinforcement Learning** ..... 3552  
Xianbo Mo (*Guangdong Key Laboratory of Intelligent Information Processing, Shenzhen Key Laboratory of Media Security, Shenzhen University*),  
Shunquan Tan (*Guangdong Key Laboratory of Intelligent Information Processing, Shenzhen Key Laboratory of Media Security, Shenzhen University*),  
Bin Li (*Guangdong Key Laboratory of Intelligent Information Processing, Shenzhen Key Laboratory of Media Security, Shenzhen University*),  
Jiwu Huang (*Guangdong Key Laboratory of Intelligent Information Processing, Shenzhen Key Laboratory of Media Security, Shenzhen University*)
- **Poster: Membership Inference Attacks via Contrastive Learning**..... 3555  
Depeng Chen (*Anhui University*), Xiao Liu (*Anhui University*), Jie Cui (*Anhui University*),  
Hong Zhong (*Anhui University*)
- **Poster: Ethics of Computer Security and Privacy Research - Trends and Standards from a Data Perspective**..... 3558  
Kevin Li (*Blue Valley Northwest High School*), Zhaohui Wang (*The University of Kansas*),  
Ye Wang (*The University of Kansas*), Bo Luo (*The University of Kansas*), Fengjun Li (*The University of Kansas*)
- **Poster: RPAL-Recovering Malware Classifiers from Data Poisoning using Active Learning**..... 3561  
Shae McFadden (*King's College London*), Zeliang Kan (*King's College London & University College London*),  
Lorenzo Cavallaro (*University College London*), Fabio Pierazzi (*King's College London*)
- **Poster: Combining Fuzzing with Concolic Execution for IoT Firmware Testing** ..... 3564  
Jihyeon Yu (*Sejong University*), Juhwan Kim (*Sejong University*),  
Yeohoon Yun (*Sejong University*), Joobeom Yun (*Sejong University*)
- **Poster: Efficient AES-GCM Decryption Under Homomorphic Encryption**..... 3567  
Ehud Aharoni (*IBM Research*), Nir Drucker (*IBM Research*), Gilad Ezov (*IBM Research*),  
Eyal Kushnir (*IBM Research*), Hayim Shaul (*IBM Research*), Omri Soceanu (*IBM Research*)
- **Poster: Multi-target & Multi-trigger Backdoor Attacks on Graph Neural Networks** ..... 3570  
Jing Xu (*Delft University of Technology*), Stjepan Picek (*Radboud University & Delft University of Technology*)
- **Poster: Longitudinal Analysis of DoS Attacks** ..... 3573  
Fabian Kaiser (*ATHENE, Fraunhofer SIT*), Haya Shulman (*ATHENE, Fraunhofer SIT, Goethe University Frankfurt*),  
Michael Waidner (*ATHENE, Fraunhofer SIT, Technical University of Darmstadt*)
- **Poster: The Risk of Insufficient Isolation of Database Transactions in Web Applications** .... 3576  
Simon Koch (*TU Braunschweig*), Malte Wessels (*TU Braunschweig*), David Klein (*TU Braunschweig*),  
Martin Johns (*TU Braunschweig*)
- **Poster: Privacy Risks from Misconfigured Android Content Providers** ..... 3579  
Christopher Lenk (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITis)*),  
Johannes Kinder (*Ludwig-Maximilians-Universität München (LMU Munich)*)
- **Poster: Bridging Trust Gaps: Data Usage Transparency in Federated Data Ecosystems**..... 3582  
Johannes Lohmöller (*RWTH Aachen University*), Eduard Vlad (*RWTH Aachen University*),  
Markus Dahlmanns (*RWTH Aachen University*), Klaus Wehrle (*RWTH Aachen University*)
- **Poster: Panacea --- Stateless and Non-Interactive Oblivious RAM** ..... 3585  
Kelong Cong (*KU Leuven*), Debajyoti Das (*KU Leuven*), Georgio Nicolas (*KU Leuven*),  
Jeongeun Park (*KU Leuven*)
- **Poster: Backdoor Attack on Extreme Learning Machines** ..... 3588  
Behrad Tajalli (*Radboud University*), Gorka Abad (*Radboud University & Ikerlan Research Centre*),  
Stjepan Picek (*Radboud University*)
- **Poster: Accountable Processing of Reported Street Problems** ..... 3591  
Roman Matzutt (*RWTH Aachen University*), Jan Pennekamp (*RWTH Aachen University*),  
Klaus Wehrle (*RWTH Aachen University*)
- **Poster: WIP: Account ZK-Rollups from Sumcheck Arguments**..... 3594  
Rex Fernando (*Carnegie Mellon University*), Arnab Roy (*Mysten Labs*)

- **Poster: Signer Discretion is Advised: On the Insecurity of Vitalik’s Threshold Hash-based Signatures** ..... 3597  
Mario Yaksetig (*University of Porto*), Alexander Havlin (*University of Manchester*)
- **Poster: Longitudinal Measurement of the Adoption Dynamics in Apple’s Privacy Label Ecosystem** ..... 3600  
David G. Balash (*University of Richmond*), Mir Masood Ali (*University of Illinois Chicago*),  
Monica Kodwani (*The George Washington University*), Xiaoyuan Wu (*Carnegie Mellon University*),  
Chris Kanich (*University of Illinois Chicago*), Adam J. Aviv (*The George Washington University*)
- **Poster: Towards a Dataset for the Discrimination between Warranted and Unwarranted Emails** ..... 3603  
Eric Burton Samuel Martin (*Colorado State University*), Hossein Shirazi (*San Deigo State University*),  
Indrakshi Ray (*Colorado State University*)
- **Poster: Cybersecurity Usage in the Wild: A look at Deployment Challenges in Intrusion Detection and Alert Handling** ..... 3606  
Wyatt Sweat (*Virginia Tech*), Danfeng (Daphne) Yao (*Virginia Tech*)
- **Poster: Towards Lightweight TEE-Assisted MPC** ..... 3609  
Wentao Dong (*City University of Hong Kong*), Cong Wang (*City University of Hong Kong*)
- **Poster: Fooling XAI with Explanation-Aware Backdoors**..... 3612  
Maximilian Noppel (*Karlsruhe Institute of Technology*), Christian Wressnegger (*Karlsruhe Institute of Technology*)
- **Poster: Metadata-private Messaging without Coordination** ..... 3615  
Peipei Jiang (*Wuhan University & City University of Hong Kong*), Qian Wang (*Wuhan University*),  
Yihao Wu (*Wuhan University*), Cong Wang (*City University of Hong Kong*)
- **Poster: Control-Flow Integrity in Low-end Embedded Devices** ..... 3618  
Sashidhar Jakkamsetti (*University of California, Irvine*), Youngil Kim (*University of California, Irvine*),  
Andrew Searles (*University of California, Irvine*), Gene Tsudik (*University of California, Irvine*)
- **Poster: Generic Multidimensional Linear Cryptanalysis of Feistel Ciphers** ..... 3621  
Betül Askin Özdemir (*KU Leuven*), Tim Beyne (*KU Leuven*)
- **Poster: Secure and Differentially Private  $k^{\text{th}}$  Ranked Element** ..... 3624  
Gowri R Chandran (*Technical University Darmstadt*),  
Philipp-Florens Lehwald (*Technical University Darmstadt*),  
Leandro Rometsch (*Technical University Darmstadt*), Thomas Schneider (*Technical University Darmstadt*)
- **Poster: Towards Practical Brainwave-based User Authentication** ..... 3627  
Matin Fallahi (*Karlsruhe Institute of Technology*), Patricia Arias-Cabarcos (*Paderborn University*),  
Thorsten Strufe (*Karlsruhe Institute of Technology*)
- **Poster: A Privacy-Preserving Smart Contract Vulnerability Detection Framework for Permissioned Blockchain**..... 3630  
Wensheng Tian (*Nanhu Lab*), Lei Zhang (*Nanhu Lab*),  
Shuangxi Chen (*Jiaxing Vocational and Technical College*),  
Hu Wang (*Zhejiang Big Data Development Administration*), Xiao Luo (*Zhejiang University*)
- **Poster: The Unknown Unknown: Cybersecurity Threats of Shadow IT in Higher Education** ..... 3633  
Jan-Philip van Acken (*Utrecht University*), Joost F. Gadellaa (*Coöperatie SURF U.A.*),  
Slinger Jansen (*Utrecht University*), Katsiaryna Labunets (*Utrecht University*)
- **Poster: Detecting Adversarial Examples Hidden under Watermark Perturbation via Usable Information Theory** ..... 3636  
Ziming Zhao (*Zhejiang University*),  
Zhaoxuan Li (*Institute of Information Engineering, Chinese Academy of Sciences*),  
Tingting Li (*Zhejiang University*), Zhuoxue Song (*Zhejiang University*), Fan Zhang (*Zhejiang University*),  
Rui Zhang (*Institute of Information Engineering, Chinese Academy of Sciences*)
- **Poster: Unveiling the Impact of Patch Placement: Adversarial Patch Attacks on Monocular Depth Estimation** ..... 3639  
Gyungeun Yun (*Korea University*), Kyunggho Joo (*Korea University*),  
Wonsuk Choi (*Korea University*), Dong Hoon Lee (*Korea University*)
- **Poster: Verifiable Data Valuation with Strong Fairness in Horizontal Federated Learning** .. 3642  
Ruei-Hau Hsu (*National Sun Yat-sen University*), Hsuan-Cheng Su (*National Sun Yat-sen University*),  
Yi-An Yu (*National Sun Yat-sen University*)

## Session 61: Workshops

- **WPES '23: 22nd Workshop on Privacy in the Electronic Society** ..... 3645  
Bart P. Knijnenburg (*Clemson University*), Panagiotis Papadimitratos (*KTH Royal Institute of Technology*)
- **CPSIoTSec'23: Fifth Workshop on CPS & IoT Security and Privacy** ..... 3648  
Magnus Almgren (*Chalmers University of Technology*), Earlene Fernandes (*University of California, San Diego*)
- **WAHC '23: 11th Workshop on Encrypted Computing & Applied Homomorphic  
Cryptography** ..... 3651  
Michael Brenner (*Leibniz Universität*),  
Anamaria Costache (*NTNU, The Norwegian University of Science and Technology*),  
Kurt Rohloff (*NJIT & Duality Technologies*)
- **MTD '23: 10th ACM Workshop on Moving Target Defense** ..... 3653  
Ning Zhang (*Washington University in St. Louis*), Qi Li (*Tsinghua University*)
- **SaTS'23: The 1st ACM Workshop on Secure and Trustworthy Superapps** ..... 3655  
Zhiqiang Lin (*The Ohio State University*), Xiaojing Liao (*Indiana University Bloomington*)
- **CCSW '23: Cloud Computing Security Workshop** ..... 3657  
Francesco Regazzoni (*University of Amsterdam & Università della Svizzera italiana*),  
Apostolos Fournaris (*Industrial Systems Institute/Research Center ATHENA*)
- **PLAS: The 18th Workshop on Programming Languages and Analysis for Security** ..... 3659  
Fraser Brown (*Carnegie Mellon University*), Klaus v. Gleissenthall (*VU Amsterdam*)
- **DeFi '23: Workshop on Decentralized Finance and Security** ..... 3660  
Kaihua Qin (*Imperial College London*), Fan Zhang (*Yale University*)
- **ARTMAN '23: First Workshop on Recent Advances in Resilient and Trustworthy  
ML Systems in Autonomous Networks** ..... 3662  
Gregory Blanc (*Telecom SudParis*),  
Takeshi Takahashi (*National Institute of Information and Communications Technology*),  
Zonghua Zhang (*Huawei Technologies France*)
- **ASHES '23: Workshop on Attacks and Solutions in Hardware Security** ..... 3664  
Lejla Batina (*Radboud University*), Chip Hong Chang (*NTU Singapore*),  
Domenic Forte (*University of Florida*), Ulrich Rübmair (*TU Berlin & U Connecticut*)
- **AISeC '23: 16th ACM Workshop on Artificial Intelligence and Security** ..... 3666  
Maura Pintor (*Università degli Studi di Cagliari*), Florian Simon Tramèr (*ETH Zurich*),  
Xinyun Chen (*Google LLC*)
- **Tutorial-HEPack4ML '23: Advanced HE Packing Methods with Applications to ML** ..... 3669  
Ehud Aharoni (*IBM Research*), Nir Drucker (*IBM Research*), Hayim Shaul (*IBM Research*)
- **SCORED '23: Workshop on Software Supply Chain Offensive Research  
and Ecosystem Defenses** ..... 3671  
Marcela Melara (*Intel Corporation*), Santiago Torres-Arias (*Purdue University*), Laurent Simon (*Google, Inc.*)

## Session 62: Demos

- **Demo: Certified Robustness on Toolformer** ..... 3673  
Yue Xu (*ShanghaiTech University*), Wenjie Wang (*ShanghaiTech University*)
- **Demo: Data Minimization and Informed Consent in Administrative Forms** ..... 3676  
Nicolas Anciaux (*Inria*), Sabine Frittella (*INSA Centre Val de Loire*),  
Baptiste Joffroy (*INSA Centre Val de Loire*), Benjamin Nguyen (*INSA Centre Val de Loire*)
- **Demo: Image Disguising for Scalable GPU-accelerated Confidential Deep Learning** ..... 3679  
Yuechun Gu (*Marquette University*), Sagar Sharma (*TikTok Inc.*), Keke Chen (*Marquette University*)

**Author Index** ..... 3682

# CCS 2023 Conference Organization

**General Chairs:** Weizhi Meng (*Technical University of Denmark*)  
Christian D. Jensen (*Technical University of Denmark*)

**Program Chairs:** Cas Cremers (*CISPA Helmholtz Center for Information Security*)  
Engin Kirda (*Khoury College of Computer Sciences*)

**Web Chairs:** Wei-Yang (Wayne) Chiu (*Technical University of Denmark*)  
Brooke Elizabeth Lampe (*Technical University of Denmark*)

**Proceedings Chairs:** Carter Yagemann (*The Ohio State University*)  
Emmanouil Vasilomanolakis (*Technical University of Denmark*)

**Sponsorship Chair:** Bo Luo (*The University of Kansas*)

**Workshop Chair:** Jun Dai (*Worcester Polytechnic Institute*)

**Poster / Demo Chair:** Sara Foresti (*University of Milan*)

**Artifact Evaluation Chair:** Thorsten Holz (*CISPA Helmholtz Center for Information Security*)

**Publicity Chairs:** Wenjuan Li (*Hong Kong Polytechnic University*)  
Rongxing Lu (*University of New Brunswick*)

**Student Travel Grant Chair:** Jun Xu (*The University of Utah*)

**Track Chairs:** Manuel Egele (*Boston University*)  
Nick Nikiforakis (*Stony Brook University*)  
Leyla Bilge (*NortonLifeLock Research Group*)  
Steve Kremer (*Inria*)  
Veelasha Moonsamy (*Ruhr University Bochum*)  
Dario Fiore (*IMDEA Software Institute*)  
Selcuk Uluagac (*Florida International University*)  
Elissa Redmiles (*Max Planck Institute*)  
Ghassan Karame (*Ruhr-University Bochum*)  
Rob Jansen (*U.S. Naval Research Laboratory*)

**Program Committee:** Tiffany Bao (*ASU*)  
Antonio Bianchi (*Purdue University*)  
Marcus Botacin (*Texas A&M University*)  
Stefan Brunthaler (*Bundeswehr University Munich*)  
Marcel Busch (*EPFL*)  
Marcel Böhme (*MPI*)  
Haipeng Cai (*Washington State University*)  
Sang Kil Cha (*KAIST*)  
Yueqi Chen (*University of Colorado - Boulder*)  
Mihai Christodorescu (*Google*)  
Daniele Cono D'Elia (*Sapienza University of Rome*)  
Ivan De Oliveira Nunes (*Rochester Institute of Technology*)  
Sevtap Duman (*Ege University*)  
Bo Feng (*Georgia Tech*)  
Guofei Gu (*TAMU*)  
Le Guan (*University of Georgia*)  
Christophe Hauser (*USC ISI*)  
Thorsten Holz (*CISPA*)  
Hong Hu (*PSU*)  
Trent Jaeger (*PSU*)  
Vasileios Kemerlis (*Brown*)  
Taesoo Kim (*Georgia Tech*)  
Christopher Kruegel (*UCSB*)  
Anil Kurmus (*IBM Research Zurich*)  
Andrea LANZI (*Università degli Studi di Milano Statale*)  
Kevin Leach (*Vanderbilt University*)  
Byoungyoung Lee (*Seoul National University*)  
Ding Li (*Peking University*)  
David Lie (*University of Toronto*)  
Christopher Liebchen (*Google*)  
Zhiqiang Lin (*Ohio State University*)  
Kangjie Lu (*University of Minnesota*)  
Aravind Machiry (*Purdue University*)  
Andrea Mambretti (*IBM Research Europe*)  
Mathias Payer (*EPFL*)  
Nuno Santos (*University of Lisbon*)  
Shweta Shinde (*ETHZ*)  
Dokyung Song (*Yonsei University*)  
Yuan Tian (*UCLA*)  
Guliz Tuncay (*Google*)  
Erik van der Kouwe (*Vrije Universiteit Amsterdam*)  
V.N. Venkatakrishnan (*UIC*)  
Alexios Voulimeneas (*KU Leuven*)

**Program Committee (continued):** Ruoyu 'Fish' Wang (*ASU*)  
Shuai Wang (*The Hong Kong University of Science and Technology*)  
Xusheng Xiao (*ASU*)  
Xinyu Xing (*Northwestern University*)  
Jun Xu (*The University of Utah*)  
Fengwei Zhang (*Southern University of Science and Technology*)  
Chao Zhang (*Tsinghua University*)  
Lianying Zhao (*Carleton University*)  
Yajin Zhou (*Zhejiang University*)  
Ali Abbasi (*CISPA*)  
Giovanni Camurati (*ETH Zurich*)  
Alvaro A. Cardenas (*University of California*)  
Gaëtan Cassiers (*TU Graz*)  
Urbi Chatterjee (*IIT Kanpur*)  
Guoxing Chen (*Shanghai Jiao Tong University*)  
Bo Chen (*Michigan Technological University*)  
Hongjun Choi (*Daegu Gyeongbuk Institute of Science and Technology*)  
Tom Chotia (*University of Birmingham*)  
Catherine Easdon (*Dynatrace Research*)  
Matthias Eckhart (*SBA Research*)  
Thomas Eisenbarth (*University of Lübeck*)  
Dmitry Evtyushkin (*William & Mary*)  
Fatemeh Ganji (*Worcester Polytechnic Institute*)  
Daniel Gruss (*TU Graz*)  
Marco Guarnieri (*IMDEA*)  
Johann Heyszl (*Google*)  
Daniel Holcomb (*UMass*)  
Mohammad A. Islam (*University of Texas at Arlington*)  
Xiaoyu Ji (*Zhejiang University*)  
Ryan Kastner (*UCSD*)  
Taegyu Kim (*Pennsylvania State University*)  
Ming Li (*University of Texas*)  
Moritz Lipp (*Amazon Web Services*)  
Mulong Luo (*Cornell University*)  
Lannan Lisa Luo (*George Mason University*)  
Michail Maniatakos (*NYU Abu Dhabi*)  
Daniel Moghimi (*Google*)  
Ben Nassi (*Ben-Gurion University*)  
Hamed Okhravi (*MIT Lincoln Laboratory*)  
Oleksii Oleksenko (*Microsoft Research Cambridge*)  
David Oswald (*University of Birmingham*)  
Norrathep Rattanavipanon (*Prince of Songkla University*)

**Program Committee (continued):** Indrakshi Ray (*Colorado State University*)  
Kaveh Razavi (*ETH Zürich*)  
Neetesh Saxena (*Cardiff University*)  
Michael Schwarz (*CISPA*)  
Riccardo Spolaor (*Shandong University*)  
Martin Strohmeier (*Armasuisse W+T*)  
Cynthia Sturton (*University of North Carolina (Chapel Hill)*)  
Petr Svenda (*Masaryk University*)  
Nils Ole Tippenhauer (*CISPA*)  
Thomas Unterluggauer (*Intel Labs*)  
Jo Van Bulck (*KU Leuven*)  
Victor van der Veen (*Qualcomm*)  
Lennert Wouters (*KU Leuven*)  
Chen Yan (*Zhejiang University*)  
Yuval Yarom (*University of Adelaide*)  
Stefano Zanero (*Politecnico di Milano*)  
Mu Zhang (*University of Utah*)  
Ziming Zhao (*University at Buffalo*)  
Ziqiao Zhou (*SR Redmond*)  
Saman Zonouz (*Georgia Tech*)  
Abbas Acar (*FIU*)  
Giovanni Apruzzese (*University of Liechtenstein*)  
Giuseppe Ateniese (*GMU*)  
Leonardo Babun (*JHUAPL*)  
Michael Backes (*CISPA*)  
Vincent Bindschaedler (*UFL*)  
Franziska Boenisch (*Vector Institute*)  
Yinzhi Cao (*JHU*)  
Berkay Celik (*Purdue University*)  
Varun Chandrasekaran (*University of Wisconsin*)  
Yizheng Chen (*UC Berkeley*)  
Kai Chen (*University of Chinese Academy of Sciences*)  
Yingying Chen (*Rutgers University*)  
Alfred Chen (*University of California*)  
Yanjiao Chen (*Zhejiang University*)  
Mauro Conti (*University of Padova*)  
Roberto Di Pietro (*HBKU-CSE*)  
Alexandra Dmitrienko (*Würzburg University*)  
Yingfei Dong (*University of Hawaii*)  
Adam Dziedzic (*Vector Institute*)  
Peng Gao (*Virginia Tech*)  
Nirnimesh Ghose (*University of Nebraska - Lincoln*)  
Neil Gong (*Duke University*)

**Program Committee (continued):** Wenbo Guo Guo (*UC Berkeley*)  
Linke Guo (*Clemson University*)  
Berk Gülmezoğlu (*Iowa State University*)  
Yuan Hong (*University of Connecticut*)  
Mathias Humbert (*Université de Lausanne*)  
Matthew Jagielski (*Google*)  
Suman Jana (*Columbia University*)  
Shouling Ji (*Zhejiang University*)  
Georgios Kambourakis (*University of the Aegean*)  
Murat Kantarcioglu (*University of Texas*)  
Koray Karabina (*National Research Council Canada*)  
Riccardo Lazzeretti (*UNIROMA*)  
Bo Li (*University of Illinois at Urbana-Champaign*)  
Ming Li (*University of Arizona*)  
Qinghua Li (*University of Arkansas*)  
Wenjing Lou (*Virginia Tech*)  
Shiqing Ma (*Rutgers University*)  
Daisuke Mashima (*Illinois at Singapore & National University of Singapore*)  
Patrick McDaniel (*University of Wisconsin*)  
Shagufta Mehnaz (*Pennsylvania State University*)  
Omid Mirzaei (*Cisco*)  
Cuong Nguyen (*FIU*)  
Anita Nikolic (*UIUC*)  
Olga Ohrimenko (*University of Melbourne*)  
Pierre Parrend (*EPITA / University of Strasbourg*)  
Thomas Pasquier (*University of British Columbia*)  
Fabio Pierazzi (*King's College London*)  
Konrad Rieck (*Technische Universität Braunschweig*)  
Ali Shahin Shamsabadi (*The Alan Turing Institute*)  
Reza Shokri (*National University of Singapore*)  
Ilia Shumailov (*University of Oxford*)  
Amit K. Sikder (*Georgia Tech*)  
Gagandeep Singh (*University of Illinois at Urbana-Champaign*)  
Ruimin Sun (*FIU*)  
Shruti Tople (*Microsoft*)  
Bimal Viswanath (*Virginia Tech*)  
Gang Wang (*University of Illinois at Urbana-Champaign*)  
Ting Wang (*Penn State*)  
Christian Wressnegger (*Karlsruhe Institute of Technology*)  
Jason Xue (*CSIRO's Data61*)  
Wei Yu (*Towson University*)



**Program Committee (continued):** Chia-Mu Yu (*National Yang Ming Chiao Tung University*)  
Xiangyu Zhang (*Purdue University*)  
Yang Zhang (*CISPA*)  
Xiao Zhang (*CISPA*)  
Hongyang Zhang (*University of Waterloo*)  
Ben Y. Zhao (*University of Chicago*)  
Sadia Afroz (*ICSI*)  
Abdelrahman Aly (*CRC - TII and imec-COSIC - KU Leuven*)  
Hassan Asghar (*Macquarie University*)  
Erman Ayday (*Case Western Reserve University*)  
Diogo Barradas (*University of Waterloo*)  
Pascal Berrang (*University of Birmingham*)  
Duc (*Snap Inc.*)  
Melissa Chase (*Microsoft Research*)  
Min Chen (*CISPA*)  
Amrita Roy Chowdhury (*UCSD*)  
Aloni Cohen (*University of Chicago*)  
Debajyoti Das (*KU Leuven*)  
Bolin Ding (*Alibaba*)  
Tariq Elahi (*University of Edinburgh*)  
Saba Eskandaria (*UNC Chapel Hill*)  
Ellis Fenske (*U.S. Naval Academy*)  
Sébastien Gambs (*Université du Québec à Montréal*)  
Emre Gürsoy (*Koç University*)  
Ryan Henry (*University of Calgary*)  
Sanghyun Hong (*Oregon State University*)  
Nicholas Hopper (*University of Minnesota*)  
Amir Houmansadr (*University of Massachusetts Amherst*)  
Aaron Johnson (*U.S. Naval Research Laboratory*)  
Marc Juarez (*University of Edinburgh*)  
Dali Kaafar (*Macquarie University*)  
Pritish Kamath (*Google*)  
Marcel Keller (*CSIRO's Data61*)  
Katharina Kohls (*Radboud University*)  
Christiane Kuhn (*NEC Laboratories Europe*)  
Wouter Lueks (*CISPA*)  
Saeed Mahloujifar (*Princeton University*)  
Anna Maria Mandalari (*Imperial College London*)  
Pasin Manurangsi (*Google*)  
Meisam Mohammady (*Iowa State University*)  
Milad Nasr (*Google Brain*)  
Joseph Near (*University of Vermont*)  
Benjamin Nguyen (*INSA Centre Val de Loire*)

**Program Committee (continued):** Rishab Nithyanand (*University of Iowa*)  
Simon Oya (*University of Waterloo*)  
Dario Pasquini (*EPFL*)  
Balazs Pejo (*BME*)  
Apostolos Pyrgelis (*EPFL*)  
Joel Reardon (*University of Calgary*)  
Thorsten Strufe (*Karlsruhe Institute of Technology*)  
Yixin Sun (*University of Virginia*)  
Michael Carl Tschantz (*ICSI*)  
Di Wang (*King Abdullah University of Science and Technology*)  
Tianhao Wang (*University of Virginia*)  
Liang Wang (*Princeton University*)  
Christian Weinert (*University of London*)  
Christopher Wood (*Cloudflare*)  
Xiaokui Xiao (*National University Singapore*)  
Arkady Yerukhimovich (*George Washington University*)  
Zhikun Zhang (*Stanford*)  
Yousra Aafer (*University of Waterloo*)  
Gunes Acar (*Radboud University*)  
Juan Caballero (*IMDEA*)  
Stefano Calzavara (*Università Ca' Foscari Venezia*)  
Niklas Carlsson (*Linköping University*)  
Aurore Fass (*Stanford*)  
Bahruz Jabiyev (*Cold Spring Harbor Laboratory*)  
Martin Johns (*TU Braunschweig*)  
Amin Kharraz (*Florida International University*)  
Pierre Laperdrix (*CNRS*)  
Xiaojing Liao (*Indiana University Bloomington*)  
Meng Luo (*Zhejiang University*)  
Wei Meng (*CUHK*)  
Shirin Nilizadeh (*UTA*)  
Giancarlo Pellegrino (*CISPA*)  
Roberto Perdisci (*University of Georgia*)  
Jason Polakis (*UIC*)  
Amir Rahmati (*Stony Brook University*)  
Tamara Rezk (*INRIA*)  
Andrei Sabelfeld (*Chalmers*)  
Merve Sahin (*SAP*)  
Brendan Saltaformaggio (*Georgia Tech*)  
Iskander Sanchez-Rola (*NortonLifeLock*)  
Anastasia Shuba (*DuckDuckGo*)  
Sooel Son (*KAIST*)  
Cristian-Alexandru Staicu (*CISPA*)

**Program Committee (continued):** Oleksii Starov (*Palo Alto Networks*)  
Phani Vadrevu (*University of New Orleans*)  
Kevin Borgolte (*Ruhr University Bochum*)  
Ang Chen (*Rice University*)  
Jianjun Chen (*Tsinghua University*)  
Jedidiah R. Crandall (*Arizona State University*)  
Lorenzo De Carli (*University of Calgary*)  
Shuang Hao (*University of Texas*)  
Wajah UI Hassan (*University of Virginia*)  
Hongxin Hu (*University of Buffalo*)  
Syed Rafiul Hussain (*PennState*)  
Mattijs Jonker (*University of Twente*)  
Min Suk Kang (*Kaist*)  
Yongdae Kim (*Kaist*)  
Platon Kotzias (*Norton Research Group*)  
Qi Li (*Tsinghua University*)  
Yao Liu (*University of South Florida*)  
Alan Zaoxing Liu (*Boston University*)  
Zhuotao Liu (*Tsinghua University*)  
Xiapu Luo (*The Hong Kong Polytechnic University*)  
Jeremiah Onalapo (*University of Vermont*)  
Michalis Polychronakis (*Stony brook University*)  
Kasper Rasmussen (*University of Oxford*)  
Chao Shen (*Jiaotong University*)  
Kun Sun (*George Mason University*)  
Andreas Terzis (*Google*)  
Ning Zhang (*Washington University St. Louis*)  
Yue Zhang (*Ohio State University*)  
Mario Alvim (*Federal University of Minas Gerais*)  
Myrto Arapinis (*University of Edinburgh*)  
Owen Arden (*UC Santa Cruz*)  
David Baelde (*ENS Rennes*)  
Musard Balliu (*KTH Royal Institute of Technology*)  
Ioana Boureanu (*University of Surrey*)  
Limin Jia (*CMU*)  
Adrien Koutsos (*INRIA Paris*)  
Matteo Maffei (*TU Wien*)  
Toby Murray (*University of Melbourne*)  
Frank Piessens (*KU Leuven*)  
Masayuki Abe (*NTT Social Informatics Laboratories*)  
Shweta Agrawal (*Indian Institute of Technology*)  
Foteini Baldimtsi (*George Mason University*)  
Manuel Barbosa (*University of Porto*)

**Program Committee (continued):** Matteo Campanelli (*Protocol Labs*)  
Dario Catalano (*University of Catania*)  
Sherman S. M. Chow (*The Chinese University of Hong Kong*)  
Anamaria Costache (*Norwegian University of Science and Technology*)  
Gareth T. Davies (*University of Wuppertal*)  
Gabrielle De Micheli (*UCSD*)  
Jean Paul Degabriele (*Technology Innovation Institute*)  
Daniel Escudero (*J.P. Morgan AI Research*)  
Sebastian Faust (*TU Darmstadt*)  
Ben Fisch (*Yale University*)  
Marc Fischlin (*TU Darmstadt*)  
Benjamin Fuller (*University of Connecticut*)  
Chaya Ganesh (*Indian Institute of Science*)  
Adria Gascon (*Google*)  
Esha Ghosh (*Microsoft Research*)  
Zichen Gui (*ETH*)  
Divya Gupta (*Microsoft Research*)  
Lucjan Hanzlik (*CISPA*)  
Tibor Jager (*University of Wuppertal*)  
Gabriel Kaptchuk (*Boston University*)  
Ngoc Khanh Nguyen (*EPFL*)  
Russell Lai (*Aalto University*)  
Kim Laine (*Microsoft Research*)  
Julian Loss (*CISPA*)  
Bernardo Magri (*The University of Manchester*)  
Antonio Marcedone (*Zoom*)  
Daniel Masny (*Meta*)  
Bart Mennink (*Radboud University*)  
Tarik Moataz (*MongoDB*)  
Pratyay Mukherjee (*SupraOracles Research*)  
Ryo Nishimaki (*NTT*)  
Anca Nitulescu (*Protocol Labs*)  
Michele Orrù (*University of Berkeley / Sorbonne University*)  
Dimitrios Papadopoulos (*University of Science and Technology*)  
Arpitra Patra (*Indian Institute of Science*)  
Giuseppe Persiano (*University of Salerno*)  
Bertram Poettering (*IBM Research Zurich*)  
Yuriy Polyakov (*Duality Technologies*)  
Antigoni Polychroniadou (*J.P. Morgan AI research*)  
Bart Preneel (*University of Leuven*)  
Mariana Raykova (*Google*)  
Christian Rechberger (*TU Graz*)

**Program Committee (continued):** Eyal Ronen (*Tel Aviv University*)  
Adeline Roux-Langlois (*IRISA*)  
Andy Rupp (*University of Luxembourg and KASTEL Security Research Labs*)  
Dominique Schröder (*Friedrich-Alexander-Universität Erlangen-Nürnberg*)  
Abhi Shelat (*Northeastern University*)  
Daniel Slamanig (*AIT Austrian Institute of Technology*)  
Yongsoo Song (*Seoul National University*)  
Ajith Suresh (*TU Darmstadt*)  
Akira Takahashi (*University of Edinburgh*)  
Sri Aravinda Krishnan Thyagarajan (*Carnegie Mellon University*)  
Ni Trieu (*Arizona State University*)  
Yiannis Tselekounis (*Carnegie Mellon University*)  
Aleksei Udovenko (*University of Luxembourg*)  
Xiao Wang (*Northwestern University*)  
David Wu (*University of Texas at Austin*)  
Jiayu Xu (*Oregon State University*)  
Bo-Yin Yang (*Academia Sinica*)  
Yu Yu (*Shanghai Jiao Tong University*)  
Greg Zaverucha (*Microsoft Research*)  
Yupeng Zhang (*Texas A&M*)  
Jiang Zhang (*State Key Laboratory of Cryptology*)  
Wenting Zheng (*CMU*)  
Ruba Abu-Salma (*Kings College London*)  
Taslima Akter (*UC Irvine*)  
Nalin Arachchilage (*University of Auckland*)  
Guangdong Bai (*University of Queensland*)  
Patricia Cabarcos (*Universität Paderborn*)  
Rahul Chatterjee (*University of Wisconsin-Madison*)  
Anupam Das (*NCSU*)  
Ali Farooq (*University of Turku*)  
Tobias Fiebig (*MPI-Inf*)  
Carlos Gañán (*ICANN*)  
Bailey Kacsmar (*U Waterloo*)  
Frank Li (*Georgia Tech*)  
Jingjie Li (*U Wisconsin-Madison*)  
Mainack Mondal (*IIT*)  
Tatsuya Mori (*Waseda University*)  
Sai Teja Peddinti (*Google*)  
Sazzadur Rahaman (*University of Arizona*)  
Nitesh Saxena (*Texas A&M*)  
Jose Such (*Kings College London*)

**Program Committee (continued):** Blase Ur (*University of Chicago*)  
Lun Wang (*Google*)  
Tina Wu (*Data61*)  
Savvas Zannettou (*TU Delft*)  
Yixin Zou (*MPI-SP*)  
Ittai Abraham (*VMWare*)  
Ghada Almashaqbeh (*University of Connecticut*)  
Frederik Armknecht (*University of Mannheim*)  
Zeta Avarikioti (*TU Wien*)  
Massimo Bartoletti (*University of Cagliari*)  
Alysson Bessani (*University of Lisbon*)  
Jing Chen (*Algorand*)  
Jeremy Clark (*Concorida*)  
Aisling Connolly (*Dfinity*)  
Lucas Davi (*University of Duisburg-Essen*)  
Sisi Duan (*Tsinghua University*)  
Stefan Dziembowski (*Warsaw*)  
Kaoutar Elkhiyaoui (*IBM Research*)  
Ittay Eyal (*Technion*)  
Yu Feng (*UCSB*)  
Peter Gazi (*IOHK*)  
Arthur Gervais (*University College London*)  
Ari Juels (*Cornell Tech*)  
Jonathan Katz (*UMD*)  
Lucianna Kiffer (*ETH Zurich*)  
Lefteris Kokoris-Kogias (*IST Austria*)  
Kari Kostinen (*ETH Zurich*)  
Ranjit Kumaresan (*Visa*)  
Duc-V Le (*Visa Research*)  
Andrew Lewis-Pye (*London School of Economics*)  
Yun Lu (*University of Victoria*)  
Giorgia Azzurra Marson (*NEC Labs*)  
Shin'ichiro Matsuo (*Georgetown University*)  
David Mohaisen (*University of Florida*)  
Pedro Moreno-Sanchez (*IMDEA*)  
Kartik Nayak (*Duke*)  
Joachim Neu (*Stanford*)  
Kirill Nikitin (*Cornell Tech*)  
Valeria Nikolaenko (*Meta*)  
Charalampos Papamanthou (*Yale*)  
Ling Ren (*UIUC*)  
Stefanie Roos (*TU Delft*)  
Stefan Schmid (*University of Vienna*)

**Program Committee (continued):** Clara Schneideweind (*MPI-SP*)  
Mark Simkin (*Ethereum*)  
Yonatan Sompolinsky (*Harvard*)  
Alberto Sonnino (*Meta*)  
Alessandro Sorniotti (*IBM Research Zurich*)  
Qiang Tang (*Sydney*)  
Karl Wuest (*CISPA*)  
Zhuolun (Daniel) Xiang (*Aptos labs*)  
Fan Zhang (*Duke*)  
Haibin Zhang (*Beijing Institute of Technology*)  
Hong-Sheng Zhou (*Virginia Commonwealth University*)  
Aviv Zohar (*HUJI*)

**Poster / Demo Committee:** Héber Arcolezi (*Inria and École Polytechnique*)  
Hafiz Asif (*Rutgers University*)  
Massimiliano Albanese (*George Mason University*)  
Enrico Bacis (*Google Zurich*)  
Joonsang Baek (*University of Wollongong*)  
Gunjan Batra (*Kennesaw State University*)  
Jonas Böhrer (*SAP*)  
Stefano Calzavara (*Università di Venezia*)  
Changlai Du (*Tianjin University*)  
Onur Duman (*Concordia University*)  
Roberto González Sánchez (*NEC Laboratories Europe*)  
Markulf Kohlweiss (*University of Edinburgh*)  
Yuan Lu (*Chinese Academy of Sciences*)  
Amir Masoumzadeh (*State University of New York*)  
Meisam Mohammady (*Iowa State University*)  
Marco Rosa (*SAP*)

## CCS 2023 Sponsor & Supporters

Sponsor:



Diamond Patron:



Platinum Patrons:



Gold Patron:



Bronze Patron:

