

2025 IEEE Symposium on Security and Privacy (SP 2025)

**San Francisco, California, USA
12-15 May 2025**

Pages 1-792



**IEEE Catalog Number: CFP25020-POD
ISBN: 979-8-3315-2237-7**

**Copyright © 2025 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP25020-POD
ISBN (Print-On-Demand):	979-8-3315-2237-7
ISBN (Online):	979-8-3315-2236-0
ISSN:	1081-6011

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2025 IEEE Symposium on Security and Privacy (SP) SP 2025

Table of Contents

Message from the Program Chairs	xxxviii
Organizing Committee	xl
Program Committee	xlii
External Reviewers	xlvi
Keynotes	1

Crime, Scams, and Fraud

SoK: Digging into the Digital Underworld of Stolen Data Markets	1
<i>Tina Marjanov (University of Cambridge, UK) and Alice Hutchings (University of Cambridge, UK)</i>	
Characterizing Robocalls with Multiple Vantage Points	19
<i>Sathvik Prasad (North Carolina State University), Aleksandr Nahapetyan (North Carolina State University), and Bradley Reaves (North Carolina State University)</i>	
Understanding the Efficacy of Phishing Training in Practice	37
<i>Grant Ho (University of Chicago and UC San Diego), Ariana Mirian (UC San Diego), Elisa Luo (UC San Diego), Khang Tong (UC San Diego Health), Euyhyun Lee (UC San Diego Health), Lin Liu (UC San Diego Health), Christopher A. Longhurst (UC San Diego Health), Christian Dameff (UC San Diego Health), Stefan Savage (UC San Diego), and Geoffrey M. Voelker (UC San Diego)</i>	
Restricting the Link: Effects of Focused Attention and Time Delay on Phishing Warning Effectiveness	55
<i>Justin Petelka (University of Washington, USA), Benjamin Berens (Karlsruhe Institute of Technology, Germany), Carlo Sugatan (University of Michigan, USA), Melanie Volkamer (Karlsruhe Institute of Technology, Germany), and Florian Schaub (University of Michigan, USA)</i>	
(Blind) Users Really Do Heed Aural Telephone Scam Warnings	N/A
<i>Filipo Sharevski (DePaul University, USA), Jennifer Vander Loop (DePaul University, USA), Bill Evans (DePaul University, USA), and Alexander Ponticello (CISPA Helmholtz Center for Information Security, Germany)</i>	

Identifying Incoherent Search Sessions: Search Click Fraud Remediation Under Real-World Constraints	93
<i>Runze Zhang (Georgia Institute of Technology), Ranjita Pai Sridhar (Microsoft Corporation), Mingxuan Yao (Georgia Institute of Technology), Zheng Yang (Georgia Institute of Technology), David Oygenblik (Georgia Institute of Technology), Haichuan Xu (Georgia Institute of Technology), Vacha Dave (Microsoft Corporation), Cormac Herley (Microsoft Corporation), Paul England (Microsoft Corporation), and Brendan Saltaformaggio (Georgia Institute of Technology)</i>	
What We Talk About When We Talk About Logs: Understanding the Effects of Dataset Quality on Endpoint Threat Detection Research	112
<i>Jason Liu (University of Illinois Urbana-Champaign), Muhammad Adil Inam (University of Illinois Urbana-Champaign), Akul Goyal (University of Illinois Urbana-Champaign), Andy Riddle (University of Illinois Urbana-Champaign), Kim Westfall (University of Illinois Urbana-Champaign), and Adam Bates (University of Illinois Urbana-Champaign)</i>	
CONnecting The EXtra doTS (CONTEXTS): Correlating External Information about Point of Interest for Attack Investigation	130
<i>Sareh Mohammadi (Concordia University, Canada), Hugo Kermabon-Bobinnec (Concordia University, Canada), Azadeh Tabiban (University of Manitoba, Canada), Lingyu Wang (Concordia University, Canada), Tomás Navarro Múnera (Concordia University, Canada), and Yosr Jarraya (Ericsson Security Research, Canada)</i>	

Threshold and Post-Quantum Cryptography

Ringtail: Practical Two-Round Threshold Signatures from Learning with Errors	149
<i>Cecilia Boschini (ETH Zürich), Darya Kaviani (UC Berkeley), Russell Lai (Aalto University), Giulio Malavolta (Bocconi University), Akira Takahashi (J.P.Morgan AI Research & AlgoCRYPT CoE), and Mehdi Tibouchi (NTT Social Informatics Laboratories)</i>	
Groundhog: A Restart-based Systems Framework for Increasing Availability in Threshold Cryptosystems	165
<i>Ashish Kashinath (University of Illinois at Urbana-Champaign), Disha Agarwala (University of Illinois at Urbana-Champaign), Gabriel Kulp (Oregon State University), Sourav Das (University of Illinois at Urbana-Champaign), Sibin Mohan (The George Washington University), and Radha Venkatagiri (Georgetown University)</i>	
Ring Referral: Efficient Publicly Verifiable Ad hoc Credential Scheme with Issuer and Strong User Anonymity for Decentralized Identity and More	184
<i>The-Anh Ta (CSIRO Data61, Australia), Xiangyu Hui (University of Melbourne, Australia), and Sid Chi-Kin Chau (CSIRO Data61, Australia)</i>	
Robust Threshold ECDSA with Online-Friendly Design in Three Rounds	203
<i>Guofeng Tang (Singapore Management University, Singapore) and Haiyang Xue (Singapore Management University, Singapore)</i>	
Security Attacks Abusing Pulse-level Quantum Circuits	222
<i>Chuanqi Xu (Yale University) and Jakub Szefer (Yale University)</i>	

Phecda: Post-Quantum Transparent zkSNARKs from Improved Polynomial Commitment and VOLE-in-the-Head with Application in Publicly Verifiable AES	240
<i>Changchang Ding (Indiana University, USA) and Yan Huang (Indiana University, USA)</i>	
Gold OPRF: Post-Quantum Oblivious Power-Residue PRF	259
<i>Yibin Yang (Georgia Institute of Technology), Fabrice Benhamouda (Amazon Web Services), Shai Halevi (Amazon Web Services), Hugo Krawczyk (Amazon Web Services), and Tal Rabin (Amazon Web Services)</i>	
Benchmarking Attacks on Learning with Errors	279
<i>Emily Wenger (Duke University, Meta AI), Eshika Saxena (Meta AI), Mohamed Malhou (Meta AI, Sorbonne Université), Ellie Thieu (University of Wisconsin - Madison), and Kristin Lauter (Meta AI)</i>	

LLM Security

Understanding Users' Security and Privacy Concerns and Attitudes Towards Conversational AI Platforms	298
<i>Mutahar Ali (University of California, Irvine, USA), Arjun Arunasalam (Purdue University, USA), and Habiba Farrukh (University of California, Irvine, USA)</i>	
On the (In)Security of LLM App Stores	317
<i>Xinyi Hou (Huazhong University of Science and Technology), Yanjie Zhao (Huazhong University of Science and Technology), and Haoyu Wang (Huazhong University of Science and Technology)</i>	
GPTracker: A Large-Scale Measurement of Misused GPTs	336
<i>Xinyue Shen (CISPA Helmholtz Center for Information Security, Germany), Yun Shen (Flexera, United Kingdom), Michael Backes (CISPA Helmholtz Center for Information Security, Germany), and Yang Zhang (CISPA Helmholtz Center for Information Security, Germany)</i>	
Modifier Unlocked: Jailbreaking Text-to-Image Models Through Prompts	355
<i>Shuofeng Liu (The University of Queensland, Australia and CSIRO's Data61, Australia), Mengyao Ma (The University of Queensland, Australia), Minhui Xue (CSIRO's Data61, Australia), and Guangdong Bai (The University of Queensland, Australia)</i>	
Fuzz-Testing Meets LLM-Based Agents: An Automated and Efficient Framework for Jailbreaking Text-To-Image Generation Models	373
<i>Yingkai Dong (School of Cyber Science and Technology, Shandong University, China), Xiangtao Meng (School of Cyber Science and Technology, Shandong University, China), Ning Yu (Netflix Eyeline Studios, USA), Zheng Li (School of Cyber Science and Technology, Shandong University, China; State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, China; Shandong Key Laboratory of Artificial Intelligence Security, Shandong University, China), and Shanqing Guo (School of Cyber Science and Technology, Shandong University, China; State Key Laboratory of Cryptography and Digital Economy Security, Shandong University, China; Shandong Key Laboratory of Artificial Intelligence Security, Shandong University, China)</i>	

On the Effectiveness of Prompt Stealing Attacks on In-The-Wild Prompts	392
<i>Yicong Tan (CISPA Helmholtz Center for Information Security), Xinyue Shen (CISPA Helmholtz Center for Information Security), Yun Shen (Flexera), Michael Backes (CISPA Helmholtz Center for Information Security), and Yang Zhang (CISPA Helmholtz Center for Information Security)</i>	
Fun-tuning: Characterizing the Vulnerability of Proprietary LLMs to Optimization-based Prompt Injection Attacks via the Fine-Tuning Interface	411
<i>Andrey Labunets (UC San Diego), Nishit Pandya (UC San Diego), Ashish Hooda (University of Wisconsin Madison), Xiaohan Fu (UC San Diego), and Earlenice Fernandes (UC San Diego)</i>	
HARMONYCLOAK: Making Music Unlearnable for Generative AI	430
<i>Syed Irfan Ali Meerza (University of Tennessee Knoxville, USA), Lichao Sun (Lehigh University), and Jian Liu (University of Tennessee Knoxville, USA)</i>	

Software Supply Chain Security

Hey, Your Secrets Leaked! Detecting and Characterizing Secret Leakage in the Wild	449
<i>Jiawei Zhou (Southeast University, China; QI-ANXIN Technology Research Institute, China), Zidong Zhang (QI-ANXIN Technology Research Institute, China), Lingyun Ying (QI-ANXIN Technology Research Institute, China), Huajun Chai (QI-ANXIN Technology Research Institute, China), Jiuxin Cao (Southeast University, China), and Haixin Duan (Quancheng Lab, China; Tsinghua University, China; Tsinghua University-QI-ANXIN Group JCNS, China)</i>	
Unveiling Security Vulnerabilities in Git Large File Storage Protocol	468
<i>Yuan Chen (Zhejiang University, China), Qinying Wang (Zhejiang University, China), Yong Yang (Zhejiang University, China), Yuanchao Chen (National University of Defense Technology, China), Yuwei Li (National University of Defense Technology, China), and Shouling Ji (Zhejiang University, China)</i>	
My Model is Malware to You: Transforming AI Models into Malware by Abusing TensorFlow APIs....	486
<i>Ruofan Zhu (Zhejiang University, China), Ganhao Chen (Zhejiang University, China), Wenbo Shen (Zhejiang University, China), Xiaofei Xie (Singapore Management University, Singapore), and Rui Chang (Zhejiang University, China)</i>	
Speedrunning the Maze: Meeting Regulatory Patching Deadlines in a Large Enterprise Environment	504
<i>Gerbrand ten Napel (Delft University of Technology, the Netherlands), Michel van Eeten (Delft University of Technology, the Netherlands), and Simon Parkin (Delft University of Technology, the Netherlands)</i>	
A Deep Dive Into How Open-Source Project Maintainers Review and Resolve Bug Bounty Reports.....	522
<i>Jessy Ayala (University of California, Irvine), Steven Ngo (University of California, Irvine), and Joshua Garcia (University of California, Irvine)</i>	

Study Club, Labor Union or Start-Up? Characterizing Teams and Collaboration in the Bug Bounty Ecosystem	539
<i>Yangheran Piao (University of Edinburgh), Temima Hrle (University of Edinburgh), Daniel Woods (University of Edinburgh, British University in Dubai), and Ross Anderson (University of Cambridge, University of Edinburgh)</i>	
CODEBREAKER: Dynamic Extraction Attacks on Code Language Models	559
<i>Changzhou Han (Swinburne University of Technology), Zehang Deng (Swinburne University of Technology), Wanlun Ma (Swinburne University of Technology), Xiaogang Zhu (The University of Adelaide), Minhui Xue (CSIRO's Data61), Tianqing Zhu (City University of Macau), Sheng Wen (Swinburne University of Technology), and Yang Xiang (Swinburne University of Technology)</i>	
Make a Feint to the East While Attacking in the West: Blinding LLM-Based Code Auditors with Flashboom Attacks	576
<i>Xiao Li (Nanjing University, China), Yue Li (Nanjing University, China), Hao Wu (Nanjing University, China), Yue Zhang (Drexel University, USA), Kaidi Xu (Drexel University, USA), Xiuzhen Cheng (Shandong University, China), Sheng Zhong (Nanjing University, China), and Fengyuan Xu (Nanjing University, China)</i>	

Keys and Passwords

Post-quantum Cryptographic Analysis of SSH	595
<i>Benjamin Benčina (Royal Holloway, University of London, UK), Benjamin Dowling (King's College London, UK), Varun Maram (SandboxAQ, UK), and Keita Xagawa (Technology Innovation Institute, UAE)</i>	
SoK: Dlog-based Distributed Key Generation	614
<i>Renas Bacho (CISPA Helmholtz Center for Information Security) and Alireza Kavousi (University College London)</i>	
Verifiable Secret Sharing Simplified	633
<i>Sourav Das (University of Illinois at Urbana Champaign), Zhuolun Xiang (Aptos Labs), Alin Tomescu (Aptos Labs), Alexander Spiegelman (Aptos Labs), Benny Pinkas (Aptos Labs, Bar-Ilan University), and Ling Ren (University of Illinois at Urbana Champaign)</i>	
Clubcards for the WebPKI: smaller certificate revocation tests in theory and practice	652
<i>John Schanck (Mozilla)</i>	
AccuRevoke: Enhancing Certificate Revocation with Distributed Cryptographic Accumulators	664
<i>Munshi Rejwan Ala Muid (Virginia Tech), Taejoong Chung (Virginia Tech), and Thang Hoang (Virginia Tech)</i>	
RankGuess: Password Guessing Using Adversarial Ranking	682
<i>Tao Yang (Nankai University, China) and Ding Wang (Nankai University, China)</i>	
Security Analysis of Master-Password-Protected Password Management Protocols	701
<i>Yihe Duan (Nankai University, China), Ding Wang (Nankai University, China), and Yanduo Fu (Nankai University, China)</i>	

Open Sesame! On the Security and Memorability of Verbal Passwords	720
<i>Eunsoo Kim (Sungkyunkwan University, South Korea), Kiho Lee (Electronics and Telecommunications Research Institute (ETRI), South Korea), Doowon Kim (University of Tennessee, United States), and Hyoungshick Kim (Sungkyunkwan University, South Korea)</i>	

Memory Safety

CMASan: Custom Memory Allocator-aware Address Sanitizer	740
<i>Junwha Hong (UNIST), Wonil Jang (UNIST), Mijung Kim (UNIST), Lei Yu (Rensselaer Polytechnic Institute), Yonghui Kwon (University of Maryland), and Yuseok Jeon (UNIST)</i>	
GoSonar: Detecting Logical Vulnerabilities in Memory Safe Language Using Inductive Constraint Reasoning	758
<i>Ma Sakib Anwar (The Ohio State University, USA), Carter Yagemann (The Ohio State University, USA), and Zhiqiang Lin (The Ohio State University, USA)</i>	
Evaluating the Effectiveness of Memory Safety Sanitizers	774
<i>Emanuel Vintila (Technical University of Munich), Philipp Zieris (Fraunhofer AISEC), and Julian Horsch (Fraunhofer AISEC)</i>	
SwiftSweeper: Defeating Use-After-Free Bugs Using Memory Sweeper Without Stop-the-World ...	793
<i>Junho Ahn (KAIST), Kanghyuk Lee (KAIST), Chanyoung Park (UNIST), Hyungon Moon (UNIST), and Youngjin Kwon (KAIST)</i>	
BridgeRouter: Automated Capability Upgrading of Out-Of-Bounds Write Vulnerabilities to Arbitrary Memory Write Primitives in the Linux Kernel	810
<i>Dongchen Xie (Renmin University of China, China), Dongnan He (Renmin University of China, China), Wei You (Renmin University of China, China), Jianjun Huang (Renmin University of China, China), Bin Liang (Renmin University of China, China), Shuitao Gan (Laboratory for Advanced Computing and Intelligence Engineering, China), and Wenchang Shi (Renmin University of China, China)</i>	
Mon CHÉRI: Mitigating Uninitialized Memory Access with Conditional Capabilities	829
<i>Merve Gülmez (Ericsson Security Research and DistriNet, KU Leuven), Håkan Englund (Ericsson Security Research), Jan Tobias Mühlberg (Université Libre de Bruxelles), and Thomas Nyman (Ericsson Product Security)</i>	
SoK: Challenges and Paths Toward Memory Safety for eBPF	848
<i>Kaiming Huang (The Pennsylvania State University), Mathias Payer (École Polytechnique Fédérale de Lausanne), Zhiyun Qian (University of California, Riverside), Jack Sampson (The Pennsylvania State University), Gang Tan (The Pennsylvania State University), and Trent Jaeger (University of California, Riverside)</i>	
IUBIK: Isolating User Bytes in Commodity Operating System Kernels via Memory Tagging Extensions	867
<i>Marius Momeu (Technical University of Munich), Alexander J. Gaidis (Brown University), Jasper v.d. Heide (Technical University of Munich), and Vasileios P. Kemerlis (Brown University)</i>	

Web Security

Predator: Directed Web Application Fuzzing for Efficient Vulnerability Validation	886
<i>Chenlin Wang (The Chinese University of Hong Kong), Wei Meng (The Chinese University of Hong Kong), Changhua Luo (The Chinese University of Hong Kong), and Penghui Li (Columbia University)</i>	
MOCGuard: Automatically Detecting Missing-Owner-Check Vulnerabilities in Java Web Applications	903
<i>Fengyu Liu (Fudan University), Youkun Shi (Fudan University), Yuan Zhang (Fudan University), Guangliang Yang (Fudan University), Enhao Li (Fudan University), and Min Yang (Fudan University)</i>	
RGFuzz: Rule-Guided Fuzzer for WebAssembly Runtimes	920
<i>Junyoung Park (KAIST), Yunho Kim (Hanyang University), and Insu Yun (KAIST)</i>	
RaceDB: Detecting Request Race Vulnerabilities in Database-Backed Web Applications	939
<i>An Chen (University of Georgia), Yonghui Kwon (University of Maryland), and Kyu Hyung Lee (University of Georgia)</i>	
PFORTIFIER: Mitigating PHP Object Injection through Automatic Patch Generation	956
<i>Bo Pang (Sichuan University, China), Yiheng Zhang (Sichuan University, China), Mingzhe Gao (Alibaba Cloud Computing, China), Junzhe Zhang (National University of Singapore, Singapore), Ligeng Chen (Nanjing University, China), Mingxue Zhang (Zhejiang University, China), and Gang Liang (Sichuan University, China)</i>	
Detecting Taint-Style Vulnerabilities in Microservice-Structured Web Applications	972
<i>Fengyu Liu (Fudan University), Yuan Zhang (Fudan University), Tian Chen (Fudan University), Youkun Shi (Fudan University), Guangliang Yang (Fudan University), Zihan Lin (Fudan University), Min Yang (Fudan University), Junyao He (Alibaba Group), and Qi Li (Alibaba Group)</i>	
Follow My Flow: Unveiling Client-Side Prototype Pollution Gadgets from One Million Real-World Websites	991
<i>Zifeng Kang (Johns Hopkins University), Muxi Lyu (Johns Hopkins University), Zhengyu Liu (Johns Hopkins University), Jianjia Yu (Johns Hopkins University), Runqi Fan (The State Key Laboratory of Blockchain and Data Security, Zhejiang University), Song Li (The State Key Laboratory of Blockchain and Data Security, Zhejiang University), and Yinzhi Cao (Johns Hopkins University)</i>	
"Only as Strong as the Weakest Link": On the Security of Brokered Single Sign-On on the Web	1009
<i>Tommaso Innocenti (Northeastern University, Boston, USA), Louis Jannett (Ruhr University Bochum, Germany), Christian Mainka (Ruhr University Bochum, Germany), Vladislav Mladenov (Ruhr University Bochum, Germany), and Engin Kirda (Northeastern University Boston, USA)</i>	

Space and Cellular Security

SoK: Space Infrastructures Vulnerabilities, Attacks and Defenses	1028
<i>Jose Luis Castanon Remy (University of Colorado Colorado Springs, USA), Ekzhin Ear (University of Colorado Colorado Springs, USA), Caleb Chang (University of Colorado Colorado Springs), Antonia Feffer (University of Colorado Colorado Springs, USA), and Shouhuai Xu (University of Colorado Colorado Springs)</i>	
Space RadSim: Binary-Agnostic Fault Injection to Evaluate Cosmic Radiation Impact on Exploit Mitigation Techniques in Space	1047
<i>Johannes Willbold (Ruhr University Bochum, Germany), Tobias Cloosters (University of Duisburg-Essen, Germany), Simon Wörner (CISPA Helmholtz Center for Information Security, Germany), Felix Buchmann (CISPA Helmholtz Center for Information Security, Germany), Moritz Schloegel (Arizona State University, USA), Lucas Davi (University of Duisburg-Essen, Germany), and Thorsten Holz (CISPA Helmholtz Center for Information Security, Germany)</i>	
Mind the Location Leakage in LEO Direct-to-Cell Satellite Networks	1064
<i>Weisen Liu (Tsinghua University, China), Zeqi Lai (Tsinghua University, China), Qian Wu (Tsinghua University, China), Hewu Li (Tsinghua University, China), Yuxuan Weng (Tsinghua University, China), Wei Liu (Tsinghua University, China), Qi Zhang (Tsinghua University, China), Jihao Li (Tsinghua University, China), Yuanjie Li (Tsinghua University, China), and Jun Liu (Tsinghua University, China)</i>	
From Control to Chaos: A Comprehensive Formal Analysis of 5G's Access Control	1081
<i>Mujtahid Akon (Pennsylvania State University), Md Toufikuzzaman (Pennsylvania State University), and Syed Rafiul Hussain (Pennsylvania State University)</i>	
BaseBridge: Bridging the Gap between Emulation and Over-The-Air Testing for Cellular Baseband Firmware	1101
<i>Daniel Klischies (Ruhr University Bochum, Germany), Dyon Goos (Vrije Universiteit Amsterdam, The Netherlands), David Hirsch (Ruhr University Bochum, Germany), Alyssa Milburn (Independent), Marius Muench (University of Birmingham, United Kingdom), and Veelasha Moonsamy (Ruhr University Bochum, Germany)</i>	
Stateful Analysis and Fuzzing of Commercial Baseband Firmware	1120
<i>Ali Ranjbar (Pennsylvania State University), Tianchang Yang (Pennsylvania State University), Kai Tu (Pennsylvania State University), Saaman Khalilollahi (Pennsylvania State University), and Syed Rafiul Hussain (Pennsylvania State University)</i>	
PGUS: Pretty Good User Security for Thick MVNOs with a Novel Sanitizable Blind Signature	1140
<i>Yang Yang (National University of Singapore, Singapore), Quan Shi (National University of Singapore, Singapore), Prosanta Gope (University of Sheffield, UK), Behzad Abdolmaleki (University of Sheffield, UK), and Biplab Sikdar (National University of Singapore, Singapore)</i>	

Invade the Walled Garden: Evaluating GTP Security in Cellular Networks	1159
<i>Yiming Zhang (Tsinghua University, China), Tao Wan (CableLabs, United States; Carleton University, Canada), Yaru Yang (Tsinghua University, China), Haixin Duan (Tsinghua University, China; Zhongguancun Laboratory, China), Yichen Wang (Tsinghua University, China), Jianjun Chen (Tsinghua University, China; Zhongguancun Laboratory, China), Zixiang Wei (Tsinghua University, China), and Xiang Li (Nankai University, China)</i>	

Privacy

SoK: A Privacy Framework for Security Research Using Social Media Data	1178
<i>Kyle Beadle (University College London), Kieron Ivy Turk (University of Cambridge), Aliai Eusebi (University College London), Mindy Tran (Max Planck Institute for Security and Privacy), Marilyne Ordekian (University College London), Enrico Mariconi (University College London), Yixin Zou (Max Planck Institute for Security and Privacy), and Marie Vasek (University College London)</i>	
GDPR in the Small: a field study of privacy and security challenges in schools	1197
<i>Francesco Ciclosi (University of Trento, Italy), Giovanna Varni (University of Trento, Italy), and Fabio Massacci (University of Trento, Italy and Vrije Universiteit, The Netherlands)</i>	
“Sorry for bugging you so much.” Exploring Developers’ Behavior Towards Privacy-Compliant Implementation	1215
<i>Stefan Albert Horstmann (Ruhr University Bochum), Sandy Hong (Ruhr University Bochum), David Klein (Technische Universität Braunschweig), Raphael Serafini (University of Cologne), Martin Degeling (Independent), Martin Johns (Technische Universität Braunschweig), Veelasha Moonsamy (Ruhr University Bochum), and Alena Naiakshina (University of Cologne)</i>	
A Low-Cost Privacy-Preserving Digital Wallet for Humanitarian Aid Distribution	1234
<i>Eva Luvison (CISPA Helmholtz Center for Information Security, Germany), Sylvain Chatel (CISPA Helmholtz Center for Information Security, Germany), Justinas Sukaitis (International Committee of the Red Cross, Switzerland), Vincent Graf Narbel (International Committee of the Red Cross, Switzerland), Carmela Troncoso (EPFL, Switzerland), and Wouter Lueks (CISPA Helmholtz Center for Information Security, Germany)</i>	
Teaching Data Science Students to Sketch Privacy Designs through Heuristics	1251
<i>Jinhe Wen (University of California, San Diego, USA), Yingxi Zhao (University of California, San Diego, USA), Wenqian Xu (University of California, San Diego, USA), Yaxing Yao (Virginia Tech, USA), and Haojian Jin (University of California, San Diego, USA)</i>	
Characterizing the Usability and Usefulness of U.S. Ad Transparency Systems	1270
<i>Kevin Bryson (University of Chicago), Arthur Borem (University of Chicago), Phoebe Moh (University of Maryland), Omer Akgul (Carnegie Mellon University), Laura Edelson (Northeastern University), Tobias Lauinger (New York University), Michelle L. Mazurek (University of Maryland), Damon McCoy (New York University), and Blase Ur (University of Chicago)</i>	

Supporting Family Discussions About Digital Privacy Through Perspective-Taking: An Empirical Investigation	1288
<i>Zikai Wen (Virginia Tech, United States), Lanjing Liu (Virginia Tech, United States), and Yaxing Yao (Virginia Tech, United States)</i>	
The Importance of Being Earnest: Shedding Light on Johnny's (False) Sense of Privacy	1306
<i>Wirawan Agahari (TU Delft, Tilburg University), Alexandra Dirksen (Technische Universitat Braunschweig), Martin Johns (Technische Universitat Braunschweig), Mark de Reuver (TU Delft), and Tobias Fiebig (Max Planck Institut fur Informatik, FG INET)</i>	

Censorship and Traffic Analysis

Learning from Censored Experiences: Social Media Discussions around Censorship Circumvention Technologies	1325
<i>Elham Pourabbas Vafa (The University of Texas at Arlington, USA), Mohit Singhal (Northeastern University, USA), Poojitha Thota (The University of Texas at Arlington, USA), and Sayak Saha Roy (The University of Texas at Arlington, USA)</i>	
Transport Layer Obscurity: Circumventing SNI Censorship on the TLS-Layer	1344
<i>Niklas Niere (Paderborn University, Germany), Felix Lange (Paderborn University, Germany), Robert Merget (Technology Innovation Institute, United Arab Emirates), and Juraj Somorovsky (Paderborn University, Germany)</i>	
A Wall Behind A Wall: Emerging Regional Censorship in China	1363
<i>Mingshi Wu (GFW Report), Ali Zohaib (University of Massachusetts Amherst), Zakir Durumeric (Stanford University), Amir Houmansadr (University of Massachusetts Amherst), and Eric Wustrow (University of Colorado Boulder)</i>	
Anix: Anonymous Blackout-Resistant Microblogging with Message Endorsing	1381
<i>Sina Kamali (University of Waterloo) and Diogo Barradas (University of Waterloo)</i>	
Is Nobody There? Good! Globally Measuring Connection Tampering without Responsive Endhosts....	1400
<i>Sadia Nourin (University of Maryland, US and Max Planck Institute for Informatics, Germany), Erik Rye (University of Maryland, USA), Kevin Bock (University of Maryland, USA), Nguyen Phong Hoang (University of British Columbia, Canada), and Dave Levin (University of Maryland, USA)</i>	
CountMamba: A Generalized Website Fingerprinting Attack via Coarse-Grained Representation and Fine-Grained Prediction	1419
<i>Xianwen Deng (Shanghai Jiao Tong University, China), Ruijie Zhao (Southeast University, China), Yanhao Wang (Independent Researcher, China), Mingwei Zhan (Shanghai Jiao Tong University, China), Zhi Xue (Shanghai Jiao Tong University, China), and Yijun Wang (Shanghai Jiao Tong University, China)</i>	

Provably Robust and Secure Steganography in Asymmetric Resource Scenarios	1438
<i>Minhao Bai (Tsinghua University), Jinshuai Yang (Tsinghua University), Kaiyi Pang (Tsinghua University), Xin Xu (Tsinghua University), Zhen Yang (Beijing University of Posts and Telecommunications), and Yongfeng Huang (Tsinghua University)</i>	
Sparta: Practical Anonymity with Long-Term Resistance to Traffic Analysis	1457
<i>Kyle Fredrickson (UC Santa Cruz), Ioannis Demertzis (UC Santa Cruz), James Hughes (UC Santa Cruz), and Darrell Long (UC Santa Cruz)</i>	

Blockchain I

P2C2T: Preserving the Privacy of Cross-Chain Transfer	1474
<i>Panpan Han (Xidian University, China), Zheng Yan (Xidian University, China), Laurence T. Yang (Zhengzhou University, China), and Elisa Bertino (Purdue University, USA)</i>	
Liquefaction: Privately Liquefying Blockchain Assets	1493
<i>James Austgen (Cornell Tech, IC3), Andrés Fábrega (Cornell Tech, IC3), Mahimna Kelkar (Cornell Tech, IC3), Dani Vilardell (Cornell Tech, IC3), Sarah Allen (IC3, Flashbots), Kushal Babel (Cornell Tech, IC3, Category Labs), Jay Yu (Stanford University), and Ari Juels (Cornell Tech, IC3)</i>	
Decentralization of Ethereum's Builder Market	1512
<i>Sen Yang (Yale University, USA), Kartik Nayak (Duke University, USA), and Fan Zhang (Yale University, USA)</i>	
A Composability Analysis Framework for Web3 Wallet Recovery Mechanisms	1531
<i>Panagiotis Chatzigiannis (Visa Research), Ke Coby Wang (Visa Research), Sunpreet Arora (Visa Research), and Mohsen Minaei (Visa Research)</i>	
Signature-Free Atomic Broadcast with Optimal $\mathcal{O}(n^2)$ Messages and $\mathcal{O}(1)$ Expected Time	1547
<i>Xiao Sui (Tsinghua University), Xin Wang (Tsinghua University), and Sisi Duan (Tsinghua University)</i>	
Warning! The Timeout T Cannot Protect You From Losing Coins PipeSwap: Forcing the Timely Release of a Secret for Atomic Cross-Chain Swaps	1566
<i>Peifang Ni (Institute of Software, Chinese Academy of Sciences; Zhongguancun Laboratory, Beijing, P.R.China), Anqi Tian (Institute of Software, Chinese Academy of Sciences; School of Computer Science and Technology, University of Chinese Academy of Sciences), and Jing Xu (Institute of Software, Chinese Academy of Sciences; School of Computer Science and Technology, University of Chinese Academy of Sciences; Zhongguancun Laboratory, Beijing, P.R.China)</i>	
Asymmetric Mempool DoS Security: Formal Definitions and Provable Secure Designs	1584
<i>Wanning Ding (Syracuse University, USA), Yuzhe Tang (Syracuse University, USA), and Yibo Wang (Syracuse University, USA)</i>	
Papercraft: Lattice-based Verifiable Delay Function Implemented	1603
<i>Michał Osadnik (Aalto University, Finland), Darya Kaviani (UC Berkeley, United States), Valerio Cini (Bocconi University, Italy), Russell W. F. Lai (Aalto University, Finland), and Giulio Malavolta (Bocconi University, Italy)</i>	

ML Attacks

Preference Poisoning Attacks on Reward Model Learning	1622
<i>Junlin Wu (Washington University in St. Louis, USA), Jiongxiao Wang (University of Wisconsin-Madison, USA), Chaowei Xiao (University of Wisconsin-Madison, USA), Chenguang Wang (Washington University in St. Louis, USA), Ning Zhang (Washington University in St. Louis, USA), and Yevgeniy Vorobeychik (Washington University in St. Louis, USA)</i>	
Query Provenance Analysis: Efficient and Robust Defense against Query-based Black-box Attacks	1641
<i>Shaofei Li (Peking University, China), Ziqi Zhang (University of Illinois Urbana-Champaign, America), Haomin Jia (Peking University, China), Yao Guo (Peking University, China), Xiangqun Chen (Peking University, China), and Ding Li (Peking University, China)</i>	
Architectural Neural Backdoors from First Principles	1657
<i>Harry Langford (University of Cambridge), Ilia Shumailov (University of Oxford), Yiren Zhao (Imperial College London), Robert Mullins (University of Cambridge), and Nicolas Papernot (University of Toronto)</i>	
BAIT: Large Language Model Backdoor Scanning by Inverting Attack Target	1676
<i>Guangyu Shen (Purdue University, USA), Siyuan Cheng (Purdue University, USA), Zhuo Zhang (Purdue University, USA), Guanhong Tao (University of Utah, USA), Kaiyuan Zhang (Purdue University, USA), Hanxi Guo (Purdue University, USA), Lu Yan (Purdue University, USA), Xiaolong Jin (Purdue University, USA), Shengwei An (Purdue University, USA), Shiqing Ma (University of Massachusetts at Amherst, USA), and Xiangyu Zhang (Purdue University, USA)</i>	
Prompt Inversion Attack against Collaborative Inference of Large Language Models	1695
<i>Wenjie Qu (National University of Singapore), Yuguang Zhou (National University of Singapore), Yongji Wu (UC Berkeley), Tingsong Xiao (University of Florida), Binhang Yuan (Hong Kong University of Science and Technology), Yiming Li (Nanyang Technological University), and Jiaheng Zhang (National University of Singapore)</i>	
PEFTGuard: Detecting Backdoor Attacks Against Parameter-Efficient Fine-Tuning	1713
<i>Zhen Sun (The Hong Kong University of Science and Technology (Guangzhou)), Tianshuo Cong (BNRist, Tsinghua University), Yule Liu (The Hong Kong University of Science and Technology (Guangzhou)), Chenhao Lin (Xi'an Jiaotong University), Xinlei He (The Hong Kong University of Science and Technology (Guangzhou)), Rongmao Chen (National University of Defense Technology), Xingshuo Han (Nanyang Technological University), and Xinyi Huang (Jinan University)</i>	

Secure Transfer Learning: Training Clean Model Against Backdoor in Pre-Trained Encoder and Downstream Dataset	1732
<i>Yechao Zhang (Huazhong University of Science and Technology, China), Yuxuan Zhou (Huazhong University of Science and Technology, China), Tianyu Li (Huazhong University of Science and Technology, China), Minghui Li (Huazhong University of Science and Technology, China), Shengshan Hu (Huazhong University of Science and Technology, China), Wei Luo (Deakin University, Australia), and Leo Yu Zhang (Griffith University, Australia)</i>	
Practical Poisoning Attacks with Limited Byzantine Clients in Clustered Federated Learning.....	1751
<i>Viet Vo (Swinburne University of Technology), Mengyao Ma (The University of Queensland), Guangdong Bai (The University of Queensland), Ryan Ko (The University of Queensland), and Surya Nepal (Data61 CSIRO)</i>	

Network Security

Beyond the Horizon: Uncovering Hosts and Services Behind Misconfigured Firewalls	1770
<i>Qing Deng (University of California, Riverside), Juefei Pu (University of California, Riverside), Zhaowei Tan (University of California, Riverside), Zhiyun Qian (University of California, Riverside), and Srikanth Krishnamurthy (University of California, Riverside)</i>	
MANTIS: Detection of Zero-Day Malicious Domains Leveraging Low Reputed Hosting Infrastructure	1789
<i>Fatih Deniz (Qatar Computing Research Institute, Qatar), Mohamed Nabeel (Palo Alto Networks Inc., USA), Ting Yu (Qatar Computing Research Institute, Qatar), and Issa Khalil (Qatar Computing Research Institute, Qatar)</i>	
Resolution Without Dissent: In-Path Per-Query Sanitization to Defeat Surreptitious Communication Over DNS	1808
<i>Daiping Liu (Palo Alto Networks, USA), Ruian Duan (Palo Alto Networks, USA), and Jun Wang (Palo Alto Networks, USA)</i>	
SoK: Decoding the Enigma of Encrypted Network Traffic Classifiers	1825
<i>Nimesha Wickramasinghe (The University of New South Wales, Australia), Arash Shaghaghi (The University of New South Wales, Australia), Gene Tsodik (University of California Irvine, USA), and Sanjay Jha (The University of New South Wales, Australia)</i>	
TrafficFormer: An Efficient Pre-trained Model for Traffic Data	1844
<i>Guangmeng Zhou (Tsinghua University, China), Xiongwen Guo (Renmin University, China), Zhuotao Liu (Tsinghua University, China; Zhongguancun Laboratory, China), Tong Li (Renmin University, China), Qi Li (Tsinghua University, China; Zhongguancun Laboratory, China), and Ke Xu (Tsinghua University, China; Zhongguancun Laboratory, China)</i>	

SCAD: Towards a Universal and Automated Network Side-Channel Vulnerability Detection	1861
<i>Keyu Man (University of California, Riverside), Zhongjie Wang (University of California, Riverside), Yu Hao (University of California, Riverside), Shenghan Zheng (University of California, Riverside), Xin'an Zhou (University of California, Riverside), Yue Cao (University of California, Riverside), and Zhiyun Qian (University of California, Riverside)</i>	
SYN Proof-of-Work: Improving Volumetric DoS Resilience in TCP	1877
<i>Samuel DeLaughter (UCSD / MIT) and Karen Sollins (MIT)</i>	
Low-cost and Robust Global Time Synchronization	1891
<i>Marc Wyss (ETH Zurich, Switzerland), Marc Frei (ETH Zurich, Switzerland), Jonghoon Kwon (ETH Zurich, Switzerland), and Adrian Perrig (ETH Zurich, Switzerland)</i>	

Blockchain II

Constant latency and finality for dynamically available DAG	1910
<i>Hans Schmiedel (The University of Sydney), Runchao Han (Babylon Labs), Qiang Tang (The University of Sydney), Ron Steinfeld (Monash University), and Jiangshan Yu (The University of Sydney)</i>	
Sailfish: Towards Improving the Latency of DAG-based BFT	1928
<i>Nibesh Shrestha (Supra Research), Rohan Shrothrium (Kuru Labs), Aniket Kate (Purdue University/Supra Research), and Kartik Nayak (Duke University)</i>	
Cauchyproofs: Batch-Updatable Vector Commitment with Easy Aggregation and Application to Stateless Blockchains	1947
<i>Zhongtang Luo (Purdue University), Yanxue Jia (Purdue University), Alejandra Gracia (No Affiliation), and Aniket Kate (Purdue University / Supra Research)</i>	
MicroNova: Folding-based arguments with efficient (on-chain) verification	1964
<i>Jiaxing Zhao (University of Science and Technology of China, China, Microsoft Research, China), Srinath Setty (Microsoft Research, USA), Weidong Cui (Microsoft Research, USA), and Greg Zaverucha (Microsoft Research, USA)</i>	
Permissionless Verifiable Information Dispersal (Data Availability for Bitcoin Rollups)	1983
<i>Ben Fisch (Yale University), Arthur Lazzaretti (Yale University), Zeyu Liu (Yale University), and Lei Yang (MIT)</i>	
An Attack on TON's ADNL Secure Channel Protocol	2002
<i>Aviv Frenkel (Fordefi, Israel) and Dmitry Kogan (Fordefi, Israel)</i>	
VITARIT: Paying for Threshold Services on Bitcoin and Friends	2018
<i>Sri AravindaKrishnan Thyagarajan (University of Sydney), Easwar Vivek Mangipudi (Supra Research), Lucjan Hanzlik (CISPA Helmholtz Center for Information Security), Aniket Kate (Purdue University/Supra Research), and Pratyay Mukherjee (Supra Research)</i>	

"Check-Before-you-Solve": Verifiable Time-lock Puzzles	2037
<i>Jiajun Xin (Hong Kong University of Science and Technology, Hong Kong SAR) and Dimitrios Papadopoulos (Hong Kong University of Science and Technology, Hong Kong SAR)</i>	

ML Defenses

Verifiable Boosted Tree Ensembles	2057
<i>Stefano Calzavara (Università Ca' Foscari Venezia, Italy), Lorenzo Cazzaro (Università Ca' Foscari Venezia, Italy), Claudio Lucchese (Università Ca' Foscari Venezia, Italy), and Giulio Ermanno Pibiri (Università Ca' Foscari Venezia, Italy)</i>	
SoK: Dataset Copyright Auditing in Machine Learning Systems	2076
<i>Linkang Du (Xi'an Jiaotong University, China), Xuanru Zhou (Zhejiang University, China), Min Chen (Vrije Universiteit Amsterdam, Netherlands), Chusong Zhang (Zhejiang University, China), Zhou Su (Xi'an Jiaotong University, China), Peng Cheng (Zhejiang University, China), Jiming Chen (Zhejiang University & Hangzhou Dianzi University, China), and Zhikun Zhang (Zhejiang University)</i>	
GRID: Protecting Training Graph from Link Stealing Attacks on GNN Models	2095
<i>Jiadong Lou (University of Delaware), Xu Yuan (University of Delaware), Rui Zhang (University of Delaware), Xingliang Yuan (The University of Melbourne), Neil Gong (Duke University), and Nian-Feng Tzeng (University of Louisiana at Lafayette)</i>	
TSQP: Safeguarding Real-Time Inference for Quantization Neural Networks on Edge Devices	2114
<i>Yu Sun (Beihang University), Gaojian Xiong (Beihang University), Jianhua Liu (Beihang University), Zheng Liu (Beihang University), and Jian Cui (Beihang University)</i>	
Fight Fire with Fire: Combating Adversarial Patch Attacks using Pattern-randomized Defensive Patches	2133
<i>Jianan Feng (Renmin University of China, China), Jiachun Li (Renmin University of China, China), Changqing Miao (Renmin University of China, China), Jianjun Huang (Renmin University of China, China), Wei You (Renmin University of China, China), Wenchang Shi (Renmin University of China, China), and Bin Liang (Renmin University of China, China)</i>	
Alleviating the Fear of Losing Alignment in LLM Fine-tuning	2152
<i>Kang Yang (University of Utah, USA), Guanhong Tao (University of Utah, USA), Xun Chen (Samsung Research America, USA), and Jun Xu (University of Utah, USA)</i>	
On the Conflict between Robustness and Learning in Collaborative Machine Learning	2171
<i>Mathilde Raynal (EPFL) and Carmela Troncoso (EPFL and MPI-SP)</i>	
DataSentinel: A Game-Theoretic Detection of Prompt Injection Attacks	2190
<i>Yupei Liu (The Pennsylvania State University), Yuqi Jia (Duke University), Jinyuan Jia (The Pennsylvania State University), Dawn Song (UC Berkeley), and Neil Zhanqiang Gong (Duke University)</i>	

Human Centered Security and Privacy I

Ownership and Gatekeeping vs. Safeguarding and Consent: How Migrant Parents Navigate Child Data Management Complexities	2209
<i>Rui Huan (University of Bristol), Kopo M. Ramokapane (University of Bristol), and Awais Rashid (University of Bristol)</i>	
“It’s time. Time for digital security.”: An End User Study on Actionable Security and Privacy Advice	2228
<i>Anna Lena Rotthaler (Paderborn University), Harshini Sri Ramulu (Paderborn University), Lucy Simko (Barnard College), Sascha Fahl (CISPA Helmholtz Center for Information Security), and Yasemin Acar (Paderborn University & The George Washington University)</i>	
“Not the Right Question?” A Study on Attitudes Toward Client-Side Scanning with Security and Privacy Researchers and a U.S. Population Sample	2246
<i>Lisa Geierhaas (University of Bonn, Germany), Florin Martius (University of Bonn, Germany), Arthi Arumugam (University of Bonn, Germany), and Matthew Smith (University of Bonn and Fraunhofer FKIE, Germany)</i>	
"Why would money protect me from cyber bullying?": A Mixed-Methods Study of Personal Cyber Insurance	2264
<i>Rachiyta Jain (University of Edinburgh, United Kingdom), Temima Hrle (University of Edinburgh, United Kingdom), Margherita Marinetti (University of Innsbruck, Austria), Adam Jenkins (King’s College London, United Kingdom), Rainer Böhme (University of Innsbruck, Austria), and Daniel W. Woods (University of Edinburgh, United Kingdom)</i>	
Security and Privacy Experiences of First- and Second-Generation Pakistani Immigrants to the US: Perceptions, Practices, Challenges, and Parent-Child Dynamics	2284
<i>Warda Usman (Brigham Young University, USA), John Sadik (The University of Tennessee, Knoxville, USA), Taha Taha (Purdue University, USA), Ran Elgedawy (The University of Tennessee, Knoxville), Scott Ruoti (The University of Tennessee, Knoxville), and Daniel Zappala (Brigham Young University, USA)</i>	
Let’s Get Visual - Testing Visual Analogies and Metaphors for Conveying Privacy Policies and Data Handling Information	2303
<i>Verena Zimmermann (ETH Zurich, Switzerland), Adrienn Toth (ETH Zurich, Switzerland), Hannah Sievers (ETH Zurich, Switzerland), Linda Fanconi (ETH Zurich, Switzerland), Yanis Isenring (ETH Zurich, Switzerland), Mona Henz (Technical University of Darmstadt, Germany), Alina Stöver (Technical University of Darmstadt, Germany), and Nina Gerber (Technical University of Darmstadt, Germany)</i>	
“I’m pretty expert and I still screw it up”: Qualitative Insights into Experiences and Challenges of Designing and Implementing Cryptographic Library APIs	2322
<i>Juliane Schmäuser (CISPA Helmholtz Center for Information Security), Philip Klostermeyer (CISPA Helmholtz Center for Information Security), Kay Friedrich (CISPA Helmholtz Center for Information Security), and Sascha Fahl (CISPA Helmholtz Center for Information Security)</i>	

“We can’t change it overnight”: Understanding Industry Perspectives on IoT Product Security Compliance and Certification	2341
<i>Prianka Mandal (William & Mary, USA) and Adwait Nadkarni (William & Mary, USA)</i>	

Secure Data Processing I

OPERA: Achieving Secure and High-performance OLAP with Parallelized Homomorphic Comparisons	2360
<i>Qi Hu (The University of Hong Kong, Hong Kong SAR, China), Wei Chen (The University of Hong Kong, Hong Kong SAR, China), Tianxiang Shen (The University of Hong Kong, Hong Kong SAR, China), Xin Yao (Huawei Technologies Co., Ltd., China), Nicholas Zhang (Huawei Technologies Co., Ltd., China), Heming Cui (The University of Hong Kong, Hong Kong SAR, China), and Siu-Ming Yiu (The University of Hong Kong, Hong Kong SAR, China)</i>	
DataSeal: Ensuring the Verifiability of Private Computation on Encrypted Data	2378
<i>Muhammad Husni Santriaji (Universitas Gadjah Mada), Jiaqi Xue (University of Central Florida), Yancheng Zhang (University of Central Florida), Qian Lou (University of Central Florida), and Yan Solihin (University of Central Florida)</i>	
CHLOE: Loop Transformation over Fully Homomorphic Encryption via Multi-Level Vectorization and Control-Path Reduction	2395
<i>Song Bian (Beihang University), Zian Zhao (Beihang University), Ruiyu Shen (Beihang University), Zhou Zhang (Beihang University), Ran Mao (Beihang University), Dawei Li (Beihang University), Yizhong Liu (Beihang University), Masaki Waga (Kyoto University), Kohei Suenaga (Kyoto University), Zhenyu Guan (Beihang University), Jiafeng Hua (Huawei Technology), Yier Jin (University of Science and Technology of China), and Jianwei Liu (Beihang University)</i>	
Improved Constructions for Distributed Multi-Point Functions	2414
<i>Elette Boyle (NTT Research and Reichman University), Niv Gilboa (Ben-Gurion University), Matan Hamilis (Reichman University), Yuval Ishai (Technion), and Yaxin Tu (Princeton University)</i>	
Preprocessing for Life: Dishonest-Majority MPC with a Trusted or Untrusted Dealer	2433
<i>Matan Hamilis (Reichman University), Elette Boyle (NTT Research and Reichman University), Niv Gilboa (Ben-Gurion University), Yuval Ishai (Technion), and Ariel Nof (Bar-Ilan University)</i>	
MatriGear: Accelerating Authenticated Matrix Triple Generation with Scalable Prime Fields via Optimized HE Packing	2453
<i>Hyunho Cha (Seoul National University), Intak Hwang (Seoul National University), Seonhong Min (Seoul National University), Jinyeong Seo (Seoul National University), and Yongsoo Song (Seoul National University)</i>	
Shark: Actively Secure Inference using Function Secret Sharing	2472
<i>Kanav Gupta (University of Maryland), Nishanth Chandran (Microsoft Research), Divya Gupta (Microsoft Research), Jonathan Katz (Google), and Rahul Sharma (Microsoft Research)</i>	

Rushing at SPDZ: On the Practical Security of Malicious MPC Implementations	2491
<i>Alexander Kyster (Aarhus University, Denmark), Frederik Huss Nielsen (Aarhus University, Denmark), Sabine Oechsner (Vrije Universiteit Amsterdam, The Netherlands), and Peter Scholl (Aarhus University, Denmark)</i>	

ML Attacks and Defenses

Rigging the Foundation: Manipulating Pre-training for Advanced Membership Inference Attacks	2509
<i>Zihao Wang (Indiana University Bloomington), Rui Zhu (Indiana University Bloomington), Zhikun Zhang (Zhejiang University), Haixu Tang (Indiana University Bloomington), and XiaoFeng Wang (Indiana University Bloomington)</i>	
Not All Edges are Equally Robust: Evaluating the Robustness of Ranking-Based Federated Learning	2527
<i>Zirui Gong (Griffith University), Yanjun Zhang (University of Technology Sydney), Leo Yu Zhang (Griffith University), Zhaoxi Zhang (University of Technology Sydney), Yong Xiang (Deakin University), and Shirui Pan (Griffith University)</i>	
Edge Unlearning is Not "on Edge"! An Adaptive Exact Unlearning System on Resource-Constrained Devices	2546
<i>Xiaoyu Xia (RMIT University, Australia), Ziqi Wang (RMIT University, Australia), Ruoxi Sun (CSIRO's Data61, Australia), Bowen Liu (Nanjing University, China), Ibrahim Khalil (RMIT University, Australia), and Minhui Xue (CSIRO's Data61, Australia)</i>	
Towards Reliable Verification of Unauthorized Data Usage in Personalized Text-to-Image Diffusion Models	2564
<i>Boheng Li (Nanyang Technological University, Singapore), Yanhao Wei (Wuhan University, China), Yankai Fu (Wuhan University, China), Zhenting Wang (Rutgers University, USA), Yiming Li (Nanyang Technological University, Singapore), Jie Zhang (CFAR and IHPC, A*STAR, Singapore), Run Wang (Wuhan University, China), and Tianwei Zhang (Nanyang Technological University, Singapore)</i>	
Watermarking Language Models for Many Adaptive Users	2583
<i>Aloni Cohen (University of Chicago, USA), Alexander Hoover (University of Chicago, USA), and Gabe Schoenbach (University of Chicago, USA)</i>	
UnMarker: A Universal Attack on Defensive Image Watermarking	2602
<i>Andre Kassis (University of Waterloo) and Urs Hengartner (University of Waterloo)</i>	
SoK: Watermarking for AI-Generated Content	2621
<i>Xuandong Zhao (UC Berkeley), Sam Gunn (UC Berkeley), Miranda Christ (Columbia University), Jaiden Fairoze (UC Berkeley), Andres Fabrega (Cornell University), Nicholas Carlini (Anthropic), Sanjam Garg (UC Berkeley), Sanghyun Hong (Oregon State University), Milad Nasr (Google DeepMind), Florian Tramèr (ETH Zurich), Somesh Jha (University of Wisconsin–Madison), Lei Li (Carnegie Mellon University), Yu-Xiang Wang (UC San Diego), and Dawn Song (UC Berkeley)</i>	

Machine Learning with Privacy for Protected Attributes	2640
<i>Saeed Mahloujifar (Meta), Chuan Guo (Meta), Edward Suh (NVIDIA), and Kamalika Chaudhuri (Meta)</i>	

Human Centered Security and Privacy II

Transparency in Usable Privacy and Security Research: Scholars' Perspectives, Practices, and Recommendations	2658
<i>Jan H. Klemmer (CISPA Helmholtz Center for Information Security, Germany), Juliane Schmäuser (CISPA Helmholtz Center for Information Security, Germany), Byron M. Lowens (University of Michigan, USA), Fabian Fischer (CISPA Helmholtz Center for Information Security, Germany), Lea Schmäuser (Leibniz University Hannover, Germany), Florian Schaub (University of Michigan, USA), and Sascha Fahl (CISPA Helmholtz Center for Information Security, Germany)</i>	
Data to Infinity and Beyond: Examining Data Sharing and Reuse Practices in the Computer Security Community	2678
<i>Anna Crowder (University of Florida, USA), Allison Lu (University of Florida, USA), Kevin Childs (University of Florida, USA), Carson Stillman (University of Florida, USA), Patrick Traynor (University of Florida, USA), and Kevin R.B. Butler (University of Florida, USA)</i>	
SoK: A Framework and Guide for Human-Centered Threat Modeling in Security and Privacy Research	2697
<i>Warda Usman (Brigham Young University, USA) and Daniel Zappala (Brigham Young University, USA)</i>	
Prevalence Overshadows Concerns? Understanding Chinese Users' Privacy Awareness and Expectations Towards LLM-based Healthcare Consultation	2716
<i>Zhihuang Liu (National University of Defense Technology, China), Ling Hu (National University of Defense Technology, China), Tongqing Zhou (National University of Defense Technology, China), Yonghao Tang (National University of Defense Technology, China), and Zhiping Cai (National University of Defense Technology, China)</i>	
Exploring Parent-Child Perspectives on Safety in Generative AI: Concerns, Mitigation Strategies, and Design Implications	2735
<i>Yaman Yu (University of Illinois Urbana-Champaign), Tanusree Sharma (Pennsylvania State University), Melinda Hu (The Hockaday School), Justin Wang (Dougherty Valley High School), and Yang Wang (University of Illinois at Urbana-Champaign)</i>	
Security Perceptions of Users in Stablecoins: Advantages and Risks within the Cryptocurrency Ecosystem	2753
<i>Maggie Yongqi Guan (University of Macau, China), Yaman Yu (University of Illinois at Urbana Champaign, USA), Tanusree Sharma (Pennsylvania State University, USA), Molly Zhuangtong Huang (University of Macau, China), Kaihua Qin (Yale University, USA), Yang Wang (University of Illinois at Urbana Champaign, USA), and Kanye Ye Wang (University of Macau, China)</i>	

Supporting Human Raters with the Detection of Harmful Content using Large Language Models 2772

Kurt Thomas (Google), Patrick Gage Kelley (Google), David Tao (Google), Sarah Meiklejohn (Google), Owen Vallis (Google), Shunwen Tan (Google), Blaž Bratanič (Google Deepmind), Felipe Tiengo Ferreira (Google Deepmind), Vijay Kumar Eranti (Google), and Elie Bursztein (Google)

"It's been lovely watching you": Institutional Decision-Making on Online Proctoring Software 2790

Elisa Shioji (University of Melbourne), Ani Meliksetyan (The George Washington University), Lucy Simko (Barnard College), Ryan Watkins (The George Washington University), Adam Aviv (The George Washington University), and Shaanan Cohnney (University of Melbourne)

Secure Data Processing II

Is MPC Secure? Leveraging Neural Network Classifiers to Detect Data Leakage Vulnerabilities in MPC Implementations 2809

Guopeng Lin (Fudan University, China), Xiaoning Du (Monash University, Australia), Lushan Song (Fudan University, China), Weili Han (Fudan University, China), Jin Tan (Ant Group, China), Junming Ma (Ant Group, China), Wenjing Fang (Ant Group, China), and Lei Wang (Ant Group, China)

Comet: Accelerating Private Inference for Large Language Model by Predicting Activation Sparsity 2827

Guang Yan (Institute of Information Engineering, Chinese Academy of Sciences), Yuhui Zhang (Institute of Information Engineering, Chinese Academy of Sciences), Zimu Guo (Institute of Information Engineering, Chinese Academy of Sciences), Lutan Zhao (Institute of Information Engineering, Chinese Academy of Sciences), Xiaojun Chen (Institute of Information Engineering, Chinese Academy of Sciences), Chen Wang (Tsinghua University, China), Wenhao Wang (Institute of Information Engineering, Chinese Academy of Sciences), Dan Meng (Institute of Information Engineering, Chinese Academy of Sciences), and Rui Hou (Institute of Information Engineering, Chinese Academy of Sciences)

Highly Efficient Actively Secure Two-Party Computation with One-Bit Advantage Bound 2846

Yi Liu (Jinan University, China), Junzuo Lai (Jinan University, China), Peng Yang (The University of Hong Kong, China), Anjia Yang (Jinan University, China), Qi Wang (Southern University of Science and Technology, China), Siu-Ming Yiu (The University of Hong Kong, China), and Jian Weng (Jinan University, China)

Hermes: Efficient and Secure Multi-Writer Encrypted Database 2865

Tung Le (Virginia Tech) and Thang Hoang (Virginia Tech)

Towards Efficient and Practical Multi-party Computation under Inconsistent Trust in TEEs 2885

Xuanwei Hu (Southern University of Science and Technology, China), Rujia Li (Tsinghua University, China), Yi Liu (Jinan University, China), and Qi Wang (Southern University of Science and Technology, China)

Hash-Prune-Invert: Improved Differentially Private Heavy-Hitter Detection in the Two-Server Model	2903
<i>Borja Balle (Google DeepMind), James Bell-Clark (Google Research), Albert Cheu (Google Research), Adria Gascon (Google Research), Jonathan Katz (Google), Mariana Raykova (Google), Phillipp Schoppmann (Google), and Thomas Steinke (Google DeepMind)</i>	
Click Without Compromise: Online Advertising Measurement via Per User Differential Privacy..	2919
<i>Yingtai Xiao (TikTok Inc., USA), Jian Du (TikTok Inc, USA), Shikun Zhang (TikTok Inc., USA), Wanrong Zhang (TikTok Inc., USA), Qiang Yan (TikTok Inc., China), Danfeng Zhang (Duke University, USA), and Daniel Kifer (The Pennsylvania State University, USA)</i>	
Smaug: Modular Augmentation of LLVM for MPC	2938
<i>Radhika Garg (Northwestern University) and Xiao Wang (Northwestern University)</i>	

Software Analysis and Reverse Engineering

Redefining Indirect Call Analysis with KallGraph	2957
<i>Guoren Li (University of California, Riverside), Manu Sridharan (University of California, Riverside), and Zhiyun Qian (University of California, Riverside)</i>	
PYLINGUAL: Toward Perfect Decompilation of Evolving High-Level Languages	2976
<i>Josh Wiedemeier (The University of Texas at Dallas), Elliot Tarbet (The University of Texas at Dallas), Max Zheng (The University of Texas at Dallas), Sangsoo Ko (The University of Texas at Dallas), Jessica Ouyang (The University of Texas at Dallas), Sang Kil Cha (Korea Advanced Institute of Science and Technology), and Kangkook Jee (The University of Texas at Dallas)</i>	
Empc: Effective Path Prioritization for Symbolic Execution with Path Cover	2995
<i>Shuangjie Yao (Hong Kong University of Science and Technology) and Dongdong She (Hong Kong University of Science and Technology)</i>	
SV-TrustEval-C: Evaluating Structure and Semantic Reasoning in Large Language Models for Source Code Vulnerability Analysis	3014
<i>Yansong Li (University of Ottawa, Canada), Paula Branco (University of Ottawa, Canada), Alexander M. Hoole (OpenText, Canada), Manish Marwah (OpenText, Canada), Hari Manassery Koduvely (OpenText, Canada), Guy-Vincent Jourdan (University of Ottawa, Canada), and Stephan Jou (OpenText, Canada)</i>	
Disassembly as Weighted Interval Scheduling with Learned Weights	3033
<i>Antonio Flores-Montoya (GrammarTech Inc.), Junghee Lim (GrammarTech Inc.), Adam Seitz (GrammarTech Inc.), Akshay Sood (GrammarTech Inc.), Edward Raff (Booz Allen Hamilton), and James Holt (Laboratory of Physical Sciences)</i>	
Inspecting Virtual Machine Diversification Inside Virtualization Obfuscation	3051
<i>Naiqian Zhang (University of New Hampshire, USA), Dongpeng Xu (University of New Hampshire, USA), Jiang Ming (Tulane University, USA), Jun Xu (University of Utah, USA), and Qiaoyan Yu (University of New Hampshire, USA)</i>	

TypeForge: Synthesizing and Selecting Best-Fit Composite Data Types for Stripped Binaries	3070
Yanzhong Wang (<i>Institute of Information Engineering, CAS, China</i>), Ruigang Liang (<i>Institute of Information Engineering, CAS, China</i>), Yilin Li (<i>Institute of Information Engineering, CAS, China</i>), Peiwei Hu (<i>Institute of Information Engineering, CAS, China</i>), Kai Chen (<i>Institute of Information Engineering, CAS, China</i>), and Bolun Zhang (<i>Institute of Information Engineering, CAS, China</i>)	
CHIMERA: Fuzzing P4 Network Infrastructure for Multi-Plane Bug Detection and Vulnerability Discovery	3088
Jiwon Kim (<i>Purdue University</i>), Dave Jing Tian (<i>Purdue University</i>), and Benjamin E. Ujcich (<i>Georgetown University</i>)	

Systems Security and Access Control

SoK: Software Compartmentalization	3107
Hugo Lefeuve (<i>The University of British Columbia</i>), Nathan Dautenhahn (<i>Serenitix</i>), David Chisnall (<i>University of Cambridge and SCI Semiconductor</i>), and Pierre Olivier (<i>The University of Manchester</i>)	
COINDEF: A Comprehensive Code Injection Defense for the Electron Framework	3127
Zheng Yang (<i>Georgia Institute of Technology, USA</i>), Simon Chung (<i>Georgia Institute of Technology, USA</i>), Jizhou Chen (<i>Georgia Institute of Technology, USA</i>), Runze Zhang (<i>Georgia Institute of Technology, USA</i>), Brendan Saltaformaggio (<i>Georgia Institute of Technology, USA</i>), and Wenke Lee (<i>Georgia Institute of Technology, USA</i>)	
Efficient Storage Integrity in Adversarial Settings	3145
Quinn Burke (<i>University of Wisconsin-Madison</i>), Ryan Sheatsley (<i>University of Wisconsin-Madison</i>), Yohan Beugin (<i>University of Wisconsin-Madison</i>), Eric Pauley (<i>University of Wisconsin-Madison</i>), Owen Hines (<i>University of Wisconsin-Madison</i>), Michael Swift (<i>University of Wisconsin-Madison</i>), and Patrick McDaniel (<i>University of Wisconsin-Madison</i>)	
Growlithe: A Developer-Centric Compliance Tool for Serverless Applications	3161
Praveen Gupta (<i>The University of British Columbia</i>), Arshia Moghimi (<i>The University of British Columbia</i>), Devam Sisodraker (<i>The University of British Columbia</i>), Mohammad Shahradd (<i>The University of British Columbia</i>), and Aastha Mehta (<i>The University of British Columbia</i>)	
The File That Contained the Keys Has Been Removed: An Empirical Analysis of Secret Leaks in Cloud Buckets and Responsible Disclosure Outcomes	3180
Soufian El Yadmani (<i>LIACS Leiden University, The Netherlands; Modat B.V., The Netherlands</i>), Olga Gadyatskaya (<i>LIACS Leiden University, The Netherlands</i>), and Yury Zhauniarovich (<i>TU Delft, The Netherlands</i>)	
EPScan: Automated Detection of Excessive RBAC Permissions in Kubernetes Applications	3199
Yue Gu (<i>Fudan University, China</i>), Xin Tan (<i>Fudan University, China</i>), Yuan Zhang (<i>Fudan University, China</i>), Siyan Gao (<i>Fudan University, China</i>), and Min Yang (<i>Fudan University, China</i>)	

403 Forbidden? Ethically Evaluating Broken Access Control in the Wild	3218
<i>Saiid El Hajj Chehade (EPFL), Florian Hantke (CISPA Helmholtz Center for Information Security), and Ben Stock (CISPA Helmholtz Center for Information Security)</i>	
“It’s almost like Frankenstein”: Investigating the Complexities of Scientific Collaboration and Privilege Management within Research Computing Infrastructures	3236
<i>Souradip Nath (Arizona State University, USA), Ananta Soneji (Arizona State University, USA), Jaeyong Baek (Arizona State University, USA), Tiffany Bao (Arizona State University, USA), Adam Doupe (Arizona State University, USA), Carlos Rubio-Medrano (Texas A&M University-Corpus Christi, USA), and Gail-Joon Ahn (Arizona State University, USA)</i>	
SoK: Integrity, Attestation, and Auditing of Program Execution	3255
<i>Mahmoud Ammar (Independent Researcher), Adam Caulfield (Rochester Institute of Technology), and Ivan De Oliveira Nunes (Rochester Institute of Technology)</i>	
The Digital Cybersecurity Expert: How Far Have We Come?	3273
<i>Dawei Wang (Zhongguancun Laboratory), Geng Zhou (Zhongguancun Laboratory), Xianglong Li (Zhongguancun Laboratory), Yu Bai (Zhongguancun Laboratory), Li Chen (Zhongguancun Laboratory), Ting Qin (Zhongguancun Laboratory), Jian Sun (Zhongguancun Laboratory), and Dan Li (Tsinghua University)</i>	

Zero Knowledge

Efficient Proofs of Possession for Legacy Signatures	3291
<i>Anna Pui Yung Woo (University of Michigan), Alex Ozdemir (Stanford University), Chad Sharp (University of Michigan), Thomas Pornin (NCC Group), and Paul Grubbs (University of Michigan)</i>	
Volatile and Persistent Memory for zkSNARKs via Algebraic Interactive Proofs	3309
<i>Alex Ozdemir (Stanford), Evan Laufer (Stanford), and Dan Boneh (Stanford)</i>	
ZHE: Efficient Zero-Knowledge Proofs for HE Evaluations	3328
<i>Zhelei Zhou (Zhejiang University), Yun Li (Ant Group), Yuchen Wang (Ant Group), Zhaomin Yang (Ant Group), Bingsheng Zhang (Zhejiang University), Cheng Hong (Ant Group), Tao Wei (Ant Group), and Wenguang Chen (Ant Group)</i>	
CoBBI: Dynamic constraint generation for SNARKs	3347
<i>Kunming Jiang (Carnegie Mellon University, USA), Fraser Brown (Carnegie Mellon University, USA), and Riad Wahby (Carnegie Mellon University, USA)</i>	
ALPACA: Anonymous Blocklisting with Constant-Sized Updatable Proofs	3364
<i>Jiwon Kim (University of Michigan), Abhiram Kothapalli (University of California, Berkeley), Orestis Chardouvelis (Carnegie Mellon University), Riad S. Wahby (Carnegie Mellon University), and Paul Grubbs (University of Michigan)</i>	

HyperPianist: Pianist with Linear-Time Prover and Logarithmic Communication Cost	3383
<i>Chongrong Li (Shanghai Jiao Tong University), Pengfei Zhu (Tsinghua University), Yun Li (Ant Group), Cheng Hong (Ant Group), Wenjie Qu (National University of Singapore), and Jiaheng Zhang (National University of Singapore)</i>	
JesseQ: Efficient Zero-Knowledge Proofs for Circuits over Any Field	3402
<i>Mengling Liu (The Hong Kong Polytechnic University), Yang Heng (The Hong Kong Polytechnic University), Xingye Lu (The Hong Kong Polytechnic University), and Man Ho Au (The Hong Kong Polytechnic University)</i>	
HydraProofs: Optimally Computing All Proofs in a Vector Commitment (with applications to efficient zkSNARKs over data from multiple users)	3421
<i>Christodoulos Pappas (Hong Kong University of Science and Technology), Dimitrios Papadopoulos (Hong Kong University of Science and Technology), and Charalampos Papamanthou (Yale University)</i>	
Zero-Knowledge Location Privacy via Accurate Floating-Point SNARKs	3440
<i>Jens Ernstberger (Technical University of Munich, Germany), Chengru Zhang (The University of Hong Kong, Hong Kong), Luca Ciprian (Technical University of Munich, Germany), Philipp Jovanovic (University College London, United Kingdom), and Sebastian Steinhorst (Technical University of Munich, Germany)</i>	
FairZK: A Scalable System to Prove Machine Learning Fairness in Zero-Knowledge	3460
<i>Tianyu Zhang (University of Illinois, Urbana-Champaign and Shanghai Jiao Tong University), Shen Dong (University of Illinois, Urbana-Champaign and Shanghai Jiao Tong University), O. Deniz Kose (University of California, Irvine), Yanning Shen (University of California, Irvine), and Yupeng Zhang (University of Illinois Urbana Champaign)</i>	

Hardware Sidechannels

Slice+Slice Baby: Generating Last-Level Cache Eviction Sets in the Blink of an Eye	3479
<i>Bradley Morgan (The University of Adelaide & Defence Science and Technology Group, Australia), Gal Horowitz (Tel-Aviv University, Israel), Sioli O'Connell (The University of Adelaide, Australia), Stephan van Schaik (University of Michigan, USA), Chitchanok Chuengsatiansup (The University of Klagenfurt, Austria), Daniel Genkin (Georgia Tech, USA), Olaf Maennel (The University of Adelaide, Australia), Paul Montague (Defence Science and Technology Group, Australia), Eyal Ronen (Tel-Aviv University, Israel), and Yuval Yarom (Ruhr University Bochum, Germany)</i>	
Rapid Reversing of Non-Linear CPU Cache Slice Functions: Unlocking Physical Address Leakage	3497
<i>Mikka Rainer (CISPA Helmholtz Center for Information Security), Lorenz Hetterich (CISPA Helmholtz Center for Information Security), Fabian Thomas (CISPA Helmholtz Center for Information Security), Tristan Hornetz (CISPA Helmholtz Center for Information Security), Leon Trampert (CISPA Helmholtz Center for Information Security), Lukas Gerlach (CISPA Helmholtz Center for Information Security), and Michael Schwarz (CISPA Helmholtz Center for Information Security)</i>	

Breaking the Barrier: Post-Barrier Spectre Attacks	3516
<i>Johannes Wikner (ETH Zurich) and Kaveh Razavi (ETH Zurich)</i>	
Peek-a-Walk: Leaking Secrets via Page Walk Side Channels	3534
<i>Alan Wang (University of Illinois at Urbana-Champaign), Boru Chen (University of California, Berkeley), Yingchen Wang (University of California, Berkeley), Christopher Fletcher (University of California, Berkeley), Daniel Genkin (Georgia Institute of Technology), David Kohlbrenner (University of Washington), and Riccardo Paccagnella (Carnegie Mellon University)</i>	
SLAP: Data Speculation Attacks via Load Address Prediction on Apple Silicon	3549
<i>Jason Kim (Georgia Tech), Daniel Genkin (Georgia Tech), and Yuval Yarom (Ruhr University Bochum)</i>	
PQ-Hammer: End-to-end Key Recovery Attacks on Post-Quantum Cryptography Using Rowhammer	3567
<i>Samy Amer (Georgia Institute of Technology, USA), Yingchen Wang (UC Berkeley, USA), Hunter Kippen (UMD and Samsung Research, USA), Thinh Dang (NIST, USA), Daniel Genkin (Georgia Institute of Technology, USA), Andrew Kwong (UNC Chapel Hill, USA), Alexander Nelson (University of Arkansas, USA), and Arkady Yerukhimovich (George Washington University, USA)</i>	
Half Spectre, Full Exploit: Hardening Rowhammer Attacks with Half Spectre Gadgets	3583
<i>Andrea Di Dio (Vrije Universiteit Amsterdam, Netherlands), Mathé Hertogh (Vrije Universiteit Amsterdam, Netherlands), and Cristiano Giuffrida (Vrije Universiteit Amsterdam, Netherlands)</i>	
Training Solo: On the Limitations of Domain Isolation Against Spectre-v2 Attacks	3599
<i>Sander Wiebing (Vrije Universiteit Amsterdam) and Cristiano Giuffrida (Vrije Universiteit Amsterdam)</i>	
Scheduled Disclosure: Turning Power Into Timing Without Frequency Scaling	3617
<i>Inwhan Chun (Carnegie Mellon University), Isabella Siu (Carnegie Mellon University), and Riccardo Paccagnella (Carnegie Mellon University)</i>	
I Know What You Sync: Covert and Side Channel Attacks on File Systems via syncfs	3636
<i>Cheng Gu (UC Riverside), Yicheng Zhang (UC Riverside), and Nael Abu-Ghazaleh (UC Riverside)</i>	

Embedded and Wireless Security

CamLoPA: A Hidden Wireless Camera Localization Framework via Signal Propagation Path Analysis	3653
<i>Xiang Zhang (University of Science and Technology of China), Jie Zhang (CFAR and IHPC, A*STAR), Zehua Ma (University of Science and Technology of China), Jinyang Huang (Hefei University of Technology), Meng Li (Hefei University of Technology), Huan Yan (Guizhou Normal University), Peng Zhao (Hefei University of Technology), Zijian Zhang (Beijing Institute of Technology), Bin Liu (University of Science and Technology of China), Qing Guo (CFAR and IHPC, A*STAR), Tianwei Zhang (Nanyang Technological University), and Nenghai Yu (University of Science and Technology of China)</i>	

Adversarial Robust ViT-based Automatic Modulation Recognition in Practical Deep Learning-based Wireless Systems	3672
<i>Gen Li (Clemson University), Chun-Chih Lin (Clemson University), Xiaonan Zhang (Florida State University), Xiaolong Ma (Clemson University), and Linke Guo (Clemson University)</i>	
SAECRED: A State-Aware, Over-the-Air Protocol Testing Approach for Discovering Parsing Bugs in SAE Handshake Implementations of COTS Wi-Fi Access Points	3691
<i>Muhammad Daniyal Pirwani Dar (Stony Brook University), Rob Lorch (The University of Iowa), Aliakbar Sadeghi (Stony Brook University), Vincenzo Sorcigli (Stony Brook University), Héloïse Gollier (DistriNet, KU Leuven), Cesare Tinelli (The University of Iowa), Mathy Vanhoef (DistriNet, KU Leuven), and Omar Chowdhury (Stony Brook University)</i>	
Your Cable, My Antenna: Eavesdropping Serial Communication via Backscatter Signals	3710
<i>Lina Pu (University of Alabama), Yu Luo (Mississippi State University), Song Han (University of Connecticut), and Junming Diao (Mississippi State University)</i>	
You Can't Judge a Binary by Its Header: Data-Code Separation for Non-Standard ARM Binaries using Pseudo Labels	3727
<i>Hadjer Benkraouda (University of Illinois Urbana-Champaign, USA), Nirav Diwan (University of Illinois Urbana-Champaign, USA), and Gang Wang (University of Illinois Urbana-Champaign, USA)</i>	
"We can't allow IoT vendors to pass off all such liability to the consumer": Investigating the U.S. Legal Perspectives on Liability for IoT Product Security	3746
<i>Prianka Mandal (William & Mary, USA), Amit Seal Ami (William & Mary, USA), Iria Giuffrida (William & Mary, USA), Daniel Shin (William & Mary, USA), Ella Sullivan (William & Mary, USA), and Adwait Nadkarni (William & Mary, USA)</i>	
PEATRS: Provable Execution in Real-Time Embedded Systems	3765
<i>Antonio Joia Neto (Rochester Institute of Technology), Norrathep Rattanavipanon (Prince of Songkla University), and Ivan De Oliveira Nunes (Rochester Institute of Technology)</i>	
FirmRCA: Towards Post-Fuzzing Analysis on ARM Embedded Firmware with Efficient Event-based Fault Localization	3783
<i>Boyu Chang (Zhejiang University), Binbin Zhao (Georgia Institute of Technology), Qiao Zhang (Zhejiang University), Peiyu Liu (Zhejiang University), Yuan Tian (University of California, Los Angeles), Raheem Beyah (Georgia Institute of Technology), and Shouling Ji (Zhejiang University)</i>	
HouseFuzz: Service-Aware Grey-Box Fuzzing for Vulnerability Detection in Linux-Based Firmware	3801
<i>Haoyu Xiao (Fudan University, China), Ziqi Wei (Fudan University, China), Jiarun Dai (Fudan University, China), Bowen Li (Fudan University, China), Yuan Zhang (Fudan University, China), and Min Yang (Fudan University, China)</i>	

Proving Faster Implementations Faster: Combining Deductive and Circuit-Based Reasoning in EasyCrypt	3820
<i>José Carlos Bacelar Almeida (Universidade do Minho and INESC TEC), Gustavo Xavier Delerue Marinho Alves (Universidade do Porto and INESC TEC and PQShield), Manuel Barbosa (Universidade do Porto (FCUP) and INESC TEC and Max Planck Institute for Security and Privacy), Gilles Barthe (Max Planck Institute for Security and Privacy and IMDEA Software Institute), Luís Esquível (Universidade do Porto (FCUP) and INESC TEC), Vincent Hwang (Max Planck Institute for Security and Privacy), Tiago Oliveira (SandboxAQ), Hugo Pacheco (Universidade do Porto (FCUP) and INESC TEC), Peter Schwabe (Max Planck Institute for Security and Privacy), and Pierre-Yves Strub (PQShield)</i>	

Differential Privacy

PAC-Private Algorithms	3839
<i>Mayuri Sridhar (Massachusetts Institute of Technology, USA), Hanshen Xiao (Purdue University/NVIDIA Research, USA), and Srinivas Devadas (Massachusetts Institute of Technology, USA)</i>	
An Attack-Agnostic Defense Framework Against Manipulation Attacks under Local Differential Privacy	3858
<i>Puning Zhao (Sun Yat-sen University), Zhikun Zhang (Zhejiang University), Jiawei Dong (Zhejiang University), Jiafei Wu (Zhejiang Lab), Shaowei Wang (Guangzhou University), Zhe Liu (Zhejiang Lab), and Yunjun Gao (Zhejiang University)</i>	
From Randomized Response to Randomized Index: Answering Subset Counting Queries with Local Differential Privacy	3877
<i>Qingqing Ye (The Hong Kong Polytechnic University), Liantong Yu (The Hong Kong Polytechnic University), Kai Huang (Macau University of Science and Technology), Xiaokui Xiao (National University of Singapore), Weiran Liu (Alibaba Group), and Haibo Hu (The Hong Kong Polytechnic University)</i>	
Augmented Shuffle Protocols for Accurate and Robust Frequency Estimation under Differential Privacy	3892
<i>Takao Murakami (The Institute of Statistical Mathematics (ISM), Japan / National Institute of Advanced Industrial Science and Technology (AIST), Japan), Yuichi Sei (The University of Electro-Communications (UEC), Japan), and Reo Eriguchi (National Institute of Advanced Industrial Science and Technology (AIST), Japan)</i>	
Differentially Private Release of Israel’s National Registry of Live Births	3912
<i>Shlomi Hod (Boston University) and Ran Canetti (Boston University)</i>	
Meeting Utility Constraints in Differential Privacy: A Privacy-Boosting Approach	3931
<i>Bo Jiang (TikTok Inc), Wanrong Zhang (TikTok Inc), Donghang Lu (TikTok Inc), Jian Du (TikTok Inc), Sagar Sharma (TikTok Inc), and Qiang Yan (TikTok Inc)</i>	
DPolicy: Managing Privacy Risks Across Multiple Releases with Differential Privacy	3950
<i>Nicolas Küchler (ETH Zürich), Alexander Viand (Intel Labs), Hidde Lycklama (ETH Zürich), and Anwar Hithnawi (University of Toronto)</i>	

Differentially Private Selection using Smooth Sensitivity	3969
<i>Iago Chaves (Universidade Federal do Ceará, Brazil), Victor Farias (Universidade Federal do Ceará, Brazil), Amanda Perez (Fundação Getulio Vargas, Brazil), Diego Mesquita (Fundação Getulio Vargas, Brazil), and Javam Machado (Universidade Federal do Ceará, Brazil)</i>	
From Easy to Hard: Building a Shortcut for Differentially Private Image Synthesis	3988
<i>Kecen Li (Institute of Automation, Chinese Academy of Sciences, China), Chen Gong (University of Virginia, USA), Xiaochen Li (University of Virginia), Yuzhong Zhao (University of Chinese Academy of Sciences), Xinwen Hou (Institute of Automation, Chinese Academy of Sciences), and Tianhao Wang (University of Virginia)</i>	
The Inadequacy of Similarity-based Privacy Metrics: Privacy Attacks against ``Truly Anonymous'' Synthetic Datasets	4007
<i>Georgi Ganev (University College London, UK and SAS Institute Inc., UK) and Emiliano De Cristofaro (University of California, Riverside, US)</i>	

Hardware Security

EUCLEAK	4026
<i>Thomas Roche (NinjaLab)</i>	
Towards ML-KEM & ML-DSA on OpenTitan	4044
<i>Amin Abdulrahman (Max Planck Institute for Security and Privacy (MPI-SP), Germany), Felix Oberhansl (Fraunhofer Institute for Applied and Integrated Security (AISEC), Germany), Hoang Nguyen Hien Pham (BULL SAS, France; Université Grenoble Alpes, France), Jade Philipoom (zeroRISC, USA), Peter Schwabe (Max Planck Institute for Security and Privacy (MPI-SP), Germany; Radboud University, The Netherlands), Tobias Stelzer (Fraunhofer Institute for Applied and Integrated Security (AISEC), Germany), and Andreas Zankl (Fraunhofer Institute for Applied and Integrated Security (AISEC), Germany)</i>	
TikTag: Breaking ARM's Memory Tagging Extension with Speculative Execution	4063
<i>Juhee Kim (Seoul National University), Jinbum Park (Samsung Research), Sihyeon Roh (Seoul National University), Jaeyoung Chung (Seoul National University), Youngjoo Lee (Seoul National University), Taesoo Kim (Samsung Research and Georgia Institute of Technology), and Byoungyoung Lee (Seoul National University)</i>	
Ceviche: Capability-Enhanced Secure Virtualization of Caches	4082
<i>Arnabjyoti Kalita (University of Virginia, USA), Yilong Yang (University of Virginia, USA), Alenkruth Krishnan Murali (University of Virginia, USA), and Ashish Venkat (University of Virginia, USA)</i>	
PORTAL: Fast and Secure Device Access with Arm CCA for Modern Arm Mobile System-on-Chips (SoCs)	4099
<i>Fan Sang (Georgia Institute of Technology), Jaehyuk Lee (Georgia Institute of Technology), Xiaokuan Zhang (George Mason University), and Taesoo Kim (Georgia Institute of Technology)</i>	

BadRAM: Practical Memory Aliasing Attacks on Trusted Execution Environments	4117
<i>Jesse De Meulemeester (KU Leuven, Belgium), Luca Wilke (University of Lübeck, Germany), David Oswald (University of Birmingham, United Kingdom), Thomas Eisenbarth (University of Lübeck, Germany), Ingrid Verbauwhede (KU Leuven, Belgium), and Jo Van Bulck (KU Leuven, Belgium)</i>	
CipherSteal: Stealing Input Data from TEE-Shielded Neural Networks with Ciphertext Side Channels	4136
<i>Yuanyuan Yuan (The Hong Kong University of Science and Technology, Hong Kong SAR, China), Zhibo Liu (The Hong Kong University of Science and Technology, Hong Kong SAR, China), Sen Deng (The Hong Kong University of Science and Technology, Hong Kong SAR, China), Yanzuo Chen (The Hong Kong University of Science and Technology, Hong Kong SAR, China), Shuai Wang (The Hong Kong University of Science and Technology, Hong Kong SAR, China), Yinqian Zhang (Southern University of Science and Technology, China), and Zhendong Su (ETH Zurich, Switzerland)</i>	
GuardAI: Protecting Emerging Generative AI Workloads on Heterogeneous NPU	4155
<i>Aritra Dhar (Computing System Lab, Huawei Zurich Research Center, Switzerland), Clément Thorens (ETH Zurich, Switzerland), Lara Magdalena Lazier (Computing System Lab, Huawei Zurich Research Center, Switzerland), and Lukas Cavigelli (Computing System Lab, Huawei Zurich Research Center, Switzerland)</i>	
TokenWeaver: Privacy Preserving and Post-Compromise Secure Attestation	4173
<i>Cas Cremers (CISPA Helmholtz Center for Information Security), Gal Horowitz (Tel Aviv University), Charlie Jacomme (Inria Nancy Grand-Est, Université de Lorraine, LORIA), and Eyal Ronen (Tel Aviv University)</i>	
IncognitOS: A Practical Unikernel Design for Full-System Obfuscation in Confidential Virtual Machines	4192
<i>Kha Dinh Duy (Sungkyunkwan University, South Korea), Jaeyoon Kim (Sungkyunkwan University, South Korea), Hajeong Lim (Sungkyunkwan University, South Korea), and Hojoon Lee (Sungkyunkwan University, South Korea)</i>	

Mobile and Smarthome Security

A Big Step Forward? A User-Centric Examination of iOS App Privacy Report and Enhancements	4210
<i>Liu Wang (Beijing University of Posts and Telecommunications, China), Dong Wang (Beijing University of Posts and Telecommunications, China), Shidong Pan (Columbia University), Zheng Jiang (Beijing University of Posts and Telecommunications, China), Haoyu Wang (Huazhong University of Science and Technology, China), and Yi Wang (Beijing University of Posts and Telecommunications, China)</i>	
Analyzing the iOS Local Network Permission from a Technical and User Perspective	4229
<i>David Schmidt (TU Wien and CDL AsTra), Alexander Ponticello (CISPA Helmholtz Center for Information Security and Saarland University), Magdalena Steinböck (TU Wien), Katharina Krombholz (CISPA Helmholtz Center for Information Security), and Martina Lindorfer (TU Wien)</i>	

WireWatch: Measuring the security of proprietary network encryption in the global Android ecosystem	4248
<i>Mona Wang (Princeton University), Jeffrey Knockel (Citizen Lab, University of Toronto), Zoë Reichert (Citizen Lab, University of Toronto), Prateek Mittal (Princeton University), and Jonathan Mayer (Princeton University)</i>	
Born with a Silver Spoon: On the (In)Security of Native Granted App Privileges in Custom Android ROMs	4267
<i>Chao Wang (Huazhong University of Science and Technology, China), Yanjie Zhao (Huazhong University of Science and Technology, China), Jiapeng Deng (Huazhong University of Science and Technology, China), and Haoyu Wang (Huazhong University of Science and Technology, China)</i>	
Code Speaks Louder: Exploring Security and Privacy Relevant Regional Variations in Mobile Applications	4284
<i>Jiawei Guo (University at Buffalo, SUNY), Yu Nong (University at Buffalo, SUNY), Zhiqiang Lin (The Ohio State University), and Haipeng Cai (University at Buffalo, SUNY)</i>	
Lombard-VLD: Voice Liveness Detection based on Human Auditory Feedback	4303
<i>Hongcheng Zhu (School of Cyber Science and Engineering, Wuhan University, China; State Grid Wuhan Electric Power Supply Company), Zongkun Sun (School of Cyber Science and Engineering, Wuhan University, China), Yanzhen Ren (School of Cyber Science and Engineering, Wuhan University, China; Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, China), Kun He (School of Cyber Science and Engineering, Wuhan University, China; Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, China), Yongpeng Yan (School of Cyber Science and Engineering, Wuhan University, China), Zixuan Wang (School of Cyber Science and Engineering, Wuhan University, China), Wuyang Liu (School of Cyber Science and Engineering, Wuhan University, China), Yuhong Yang (National Engineering Research Center for Multimedia Software, School of Computer Science, Wuhan University; Hubei Key Laboratory of Multimedia and Network Communication Engineering, China), and Weiping Tu (National Engineering Research Center for Multimedia Software, School of Computer Science, Wuhan University; Hubei Key Laboratory of Multimedia and Network Communication Engineering, China)</i>	
Analyzing Ad Prevalence, Characteristics, and Compliance in Alexa Skills	4321
<i>Aafaq Sabir (North Carolina State University, USA), Abhinaya S.B. (North Carolina State University, USA), Dilawer Ahmed (North Carolina State University, USA), and Anupam Das (North Carolina State University, USA)</i>	
Eyes on Your Typing: Snooping Finger Motions on Virtual Keyboards	4340
<i>Sunwoo Lee (Seoul Women's University) and Wonsuk Choi (Korea University)</i>	

BPSniff: Continuously Surveilling Private Blood Pressure Information in the Metaverse via Unrestricted Inbuilt Motion Sensors	4356
<i>Zhengkun Ye (Temple University), Ahmed Tanvir Mahdad (Texas A&M University, College Station), Yan Wang (Temple University), Cong Shi (New Jersey Institute of Technology), Yingying Chen (Rutgers University), and Nitesh Saxena (Texas A&M University, College Station)</i>	

Private and Secure Communication

TreeKEM: A Modular Machine-Checked Symbolic Security Analysis of Group Key Agreement in Messaging Layer Security	4375
<i>Théophile Wallez (Inria Paris), Jonathan Protzenko (Microsoft Azure Research), and Karthikeyan Bhargavan (Cryspen)</i>	
Impossibility Results for Post-Compromise Security in Real-World Communication Systems	4391
<i>Cas Cremers (CISPA Helmholtz Center for Information Security), Niklas Medinger (CISPA Helmholtz Center for Information Security), and Aurora Naska (CISPA Helmholtz Center for Information Security)</i>	
Extended Diffie-Hellman Encryption for Secure and Efficient Real-Time Beacon Notifications.....	4406
<i>Liron David (Weizmann Institute of Science and Google), Omer Berkman (The Academic College of Tel Aviv-Yaffo and Google), Avinatan Hassidim (Bar Ilan University and Google), David Lazarov (Google), Yossi Matias (Tel-Aviv University and Google), and Moti Yung (Columbia University and Google)</i>	
Myco: Unlocking Polylogarithmic Accesses in Metadata-Private Messaging	4419
<i>Darya Kaviani (University of California, Berkeley), Deevoashwer Rathee (University of California, Berkeley), Bhargav Annem (California Institute of Technology), and Raluca Ada Popa (University of California, Berkeley)</i>	
Peer2PIR: Private Queries for IPFS	4438
<i>Miti Mazmudar (University of Waterloo), Shannon Veitch (ETH Zurich), and Rasoul Akhavan Mahdavi (University of Waterloo)</i>	
Mixnets on a tightrope: Quantifying the leakage of mix networks using a provably optimal heuristic adversary	4457
<i>Sebastian Meiser (University of Luebeck, Germany), Debajyoti Das (Umea University, Sweden), Moritz Kirschte (University of Luebeck, Germany), Esfandiar Mohammadi (University of Luebeck, Germany), and Aniket Kate (Purdue University & Supra Research, USA)</i>	
TreePIR: Efficient Private Retrieval of Merkle Proofs via Tree Colorings with Fast Indexing and Zero Storage Overhead	4476
<i>Quang Cao (RMIT University), Son Hoang Dau (RMIT University), Rinaldo Gagliano (RMIT University), Duy Huynh (RMIT University), Xun Yi (RMIT University), Phuc Lu Le (University of Science - VNU-HCM), Quang-Hung Luu (Bureau of Meteorology), Emanuele Viterbo (Monash University), Yu-Chih Huang (National Yang Ming Chiao Tung University), Jingge Zhu (University of Melbourne), Mohammad M. Jalalzai (University of British Columbia (Okanagan Campus)), and Chen Feng (University of British Columbia (Okanagan Campus))</i>	

SoK: Self-Generated Nudes over Private Chats: How Can Technology Contribute to a Safer Sexting?	4495
<i>Joel Samper (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal) and Bernardo Ferreira (LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal)</i>	
"You Have to Ignore the Dangers": User Perceptions of the Security and Privacy Benefits of WhatsApp Mods	4515
<i>Collins W. Munyendo (The George Washington University), Kentrell Owens (University of Washington), Faith Strong (Austin College), Shaoqi Wang (University of Washington), Adam J. Aviv (The George Washington University), Tadayoshi Kohno (University of Washington), and Franziska Roesner (University of Washington)</i>	

Audio and Video Security

EveGuard: Defeating Vibration-based Side-Channel Eavesdropping with Audio Adversarial Perturbations	4534
<i>Jung-Woo Chang (University of California, San Diego), Ke Sun (University of Michigan, Ann Arbor), David Xia (University of Illinois Urbana-Champaign), Xinyu Zhang (University of California, San Diego), and Farinaz Koushanfar (University of California, San Diego)</i>	
Spoofing Eavesdroppers with Audio Misinformation	4553
<i>Zhambyl Shaikhanov (University of Maryland - College Park, USA), Mahmoud Al-Madi (Rice University, USA), Hou-Tong Chen (Los Alamos National Laboratory, USA), Chun-Chieh Chang (Los Alamos National Laboratory, USA), Sadhvikas Addamane (Sandia National Laboratories, USA), Daniel M. Mittleman (Brown University, USA), and Edward Knightly (Rice University, USA)</i>	
EvilHarmony: Stealthy Adversarial Attacks against Black-box Speech Recognition Systems	4569
<i>Xuejing Yuan (School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China; State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, Beijing, China), Jiangshan Zhang (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, Beijing, China; School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China), Feng Guo (School of Cyber Science and Technology, Shandong University, Qingdao, China), Kai Chen (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, Beijing, China; School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China), XiaoFeng Wang (Indiana University Bloomington, USA), Shengzhi Zhang (Metropolitan College, Boston University, Boston, USA), Yuxuan Chen (School of Cyber Science and Technology, Shandong University, Qingdao, China; Quancheng Laboratory, Jinan, China), Dun Liu (Metropolitan College, Boston University, Boston, USA), Pan Li (State Key Laboratory of Cyberspace Security Defense, Institute of Information Engineering, CAS, Beijing, China; School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China), Zihao Wang (Indiana University Bloomington, USA), and Runnan Zhu (School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China)</i>	

Investigating Physical Latency Attacks against Camera-based Perception	4588
<i>Raymond Muller (Purdue University), Ruoyu Song (Purdue University), Chenyi Wang (University of Arizona), Yuxia Zhan (New York University), Jean-Philippe Monteuis (Qualcomm Technologies Inc.), Yanmao Man (HERE Technologies, Inc.), Ming Li (University of Arizona), Ryan Gerdes (Virginia Tech), Jonathan Petit (Qualcomm), and Z. Berkay Celik (Purdue University)</i>	
VerITAS: Verifying Image Transformations at Scale	4606
<i>Trisha Datta (Stanford University, USA), Binyi Chen (Stanford University, USA), and Dan Boneh (Stanford University, USA)</i>	
Trust Nobody: Privacy-Preserving Proofs for Edited Photos with Your Laptop	4624
<i>Pierpaolo Della Monica (Sapienza University of Rome, Italy), Ivan Visconti (Sapienza University of Rome, Italy), Andrea Vitaletti (Sapienza University of Rome, Italy), and Marco Zecchini (Sapienza University of Rome, Italy)</i>	
Eva: Efficient Privacy-Preserving Proof of Authenticity for Lossily Encoded Videos	4643
<i>Chengru Zhang (The University of Hong Kong, Hong Kong), Xiao Yang (University of Birmingham, UK), David Oswald (University of Birmingham, UK), Mark Ryan (University of Birmingham, UK), and Philipp Jovanovic (University College London, UK)</i>	
From One Stolen Utterance: Assessing the Risks of Voice Cloning in the AIGC Era	4663
<i>Kun Wang (Zhejiang University, China), Meng Chen (Zhejiang University, China), Li Lu (Zhejiang University, China), Jingwen Feng (Zhejiang University, China), Qianniu Chen (Zhejiang University, China), Zhongjie Ba (Zhejiang University, China), Kui Ren (Zhejiang University, China), and Chun Chen (Zhejiang University, China)</i>	
Sniffing Location Privacy of Video Conference Users Using Free Audio Channels	4682
<i>Long Huang (Southern Methodist University, USA) and Chen Wang (Southern Methodist University, USA)</i>	

Author Index