TUESDAY

7:30	**Registration & Breakfast**				
9:00	**Chairs' Welcome (Kings)**				
9:15	**Keynote: Ingrid Verbauwhede - The Need for Hardware Roots of Trust (Kings)**				
10:30	**Coffee Break**				
	Kings - Balmoral	**Kings - Sandringham**	**Windsor**	**Blenheim**	**Buckingham**
11:00	**Session 1A: Attacks I** *Chair: Wenyuan Xu*	**Session 1B: Cryptographic Primitives** *Chair: Dario Fiore*	**Session 1C: Cloud Security I** *Chair: Zhiqiang Lin*	**Session 1D: Forensics** *Chair: Omar Chowdhury*	**Session 1E: Privacy I** *Chair: Ben Stock*
	1 Trillion Dollar Refund - How To Spoof PDF Signatures *Vladislav Mladenov (Ruhr University Bochum),Christian Mainka (Ruhr University Bochum),Karsten Meyer zu Selhausen (Hackmanit GmbH),Martin Grothe (Ruhr University Bochum),Jörg Schwenk (Ruhr University Bochum)*	Omniring: Scaling Up Private Payments Without Trusted Setup - Formal Foundations and a Construction of Ring Confidential Transactions with Log-size Proofs *Russell W. F. Lai (Friedrich Alexander University Erlangen-Nuremberg),Viktoria Ronge (Friedrich Alexander University Erlangen-Nuremberg),Tim Ruffing (Blockstream),Dominique Schröder (Friedrich Alexander University Erlangen-Nuremberg),Sri Aravinda Krishnan Thyagarajan (Friedrich Alexander University Erlangen-Nuremberg),Jiafan Wang (Chinese University of Hong Kong)*	A Machine-Checked Proof of Security for AWS Key Management Service *José Bacelar Almeida (University of Minho and INESC TEC),Manuel Barbosa (University of Porto (FCUP) and INESC TEC),Gilles Barthe (MPI-SP and IMDEA Software Institute),Matthew Campagna (Amazon Web Services),Ernie Cohen (Amazon Web Services),Benjamin Gregoire (INRIA Sophia Antipolis),Vitor Pereira (University of Porto (FCUP) and INESC TEC),Bernardo Portela (University of Porto (FCUP) and INESC TEC),Pierre-Yves Strub (École Polytechnique),Serdar Tasiran (Amazon Web Services)*	The Next 700 Policy Miners: A Universal Method for Building Policy Miners *Carlos Cotrini (ETH Zurich),Luca Corinzia (ETH Zurich),Thilo Weghorn (ETH Zurich),David Basin (ETH Zurich)*	Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices *Hooman Mohajeri Moghaddam (Princeton University),Gunes Acar (Princeton University),Arunesh Mathur (Princeton University),Danny Y. Huang (Princeton University),Ben Burgess (Princeton University),Nick Feamster (Princeton University),Edward Felten (Princeton University),Prateek Mittal (Princeton University),Arvind Narayanan (Princeton University)*
	Practical Decryption exFiltration: Breaking PDF Encryption *Jens Müller (Ruhr University Bochum),Fabian Ising (Münster University of Applied Sciences),Vladislav Mladenov (Ruhr University Bochum),Christian Mainka (Ruhr University Bochum),Sebastian Schinzel (Münster University of Applied Sciences),Jörg Schwenk (Ruhr University Bochum)*	WI is not Enough: Zero-Knowledge Contingent (Service) Payments Revisited *Georg Fuchsbauer (Inria and Ecole normale superieure)*	Mitigating Leakage in Secure Cloud-Hosted Data Structures: Volume Hiding for Multi-Maps via Hashing *Sarvar Patel (Google),Giuseppe Persiano (Universita' di Salerno and Google),Kevin Yeo (Google),Moti Yung (Google)*	Towards Continuous Access Control Validation and Forensics *Chengcheng Xiang, Yudong Wu, Bingyu Shen, Mingyao Shen (University of California San Diego),Tianyin Xu (University of Illinois Urbana-Champaign),Yuanyuan Zhou, Cindy Moore (University of California San Diego),Xinxin Jin,Tianwei Sheng (Whova, Inc.)*	Oh, the Places You've Been! User Reactions to Longitudinal Transparency About Third-Party Web Tracking and Inferencing *Ben Weinshel,Miranda Wei (University of Chicago),Mainack Mondal (Cornell University / University of Chicago),Euirim Choi,Shawn Shan,Claire Dolin (University of Chicago),Michelle L. Mazurek (University of Maryland),Blase Ur (University of Chicago)*
12:00	**Lunch Break (Monarch)**				
13:30	**Session 2A: Side Channels I** *Chair: Michael Franz*	**Session 2B: ML Security I** *Chair: Yang Zhang*	**Session 2C: Secure Computing I** *Chair: Yan Huang*	**Session 2D: Encryption (Searchable, Updatable, Homomorphic, etc.)** *Chair: Joshua Schiffman*	**Session 2E: Internet Security** *Chair: Paul Pearce*
	Page Cache Attacks *Daniel Gruss (Graz University of Technology),Erik Kraft (Graz University of Technology),Trishita Tiwari (Boston University),Michael Schwarz (Graz University of Technology),Ari Trachtenberg (Boston University),Jason Hennessey (NetApp),Alex Ionescu (CrowdStrike),Anders Fogh (Intel Corporation)*	Neural Network Inversion in Adversarial Setting via Background Knowledge Alignment *Ziqi Yang (National University of Singapore),Jiyi Zhang (National University of Singapore),Ee-Chien Chang (National University of Singapore),Zhenkai Liang (National University of Singapore)*	Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation *Elette Boyle (IDC Herzliya),Geoffroy Couteau (Karlsruhe Institute of Technology),Niv Gilboa (Ben-Gurion University of the Negev),Yuval Ishai (Technion),Lisa Kohl (Karlsruhe Institute of Technology),Peter Rindal (Visa Research),Peter Scholl (Aarhus University)*	Encrypted Databases: New Volume Attacks against Range Queries *Zichen Gui (University of Bristol),Oliver Johnson (University of Bristol),Bogdan Warinschi (University of Bristol)*	SICO: Surgical Interception Attacks by Manipulating BGP Communities *Henry Birge-Lee (Princeton University),Liang Wang (Princeton University),Jennifer Rexford (Princeton University),Prateek Mittal (Princeton University)*
	Hardware-Backed Heist: Extracting ECDSA Keys from Qualcomm's TrustZone *Keegan Ryan (NCC Group)*	Privacy Risks of Securing Machine Learning Models against Adversarial Examples *Liwei Song (Princeton University),Reza Shokri (National University of Singapore (NUS)),Prateek Mittal (Princeton University)*	Endemic Oblivious Transfer *Peter Rindal (Visa Research),Daniel Masny (Visa Research)*	Updatable Oblivious Key Management for Storage Systems *Stanislaw Jarecki (University of California, Irvine),Hugo Krawczyk (Algorand Foundation),Jason Resch (Independent)*	Just the Tip of the Iceberg: Internet-Scale Exploitation of Routers for Cryptojacking *H.L.J. Bijmans (Delft University of Technology),T.M. Booij (Delft University of Technology),C. Doerr (Delft University of Technology)*
	VoltJockey: Breaching TrustZone by Software-Controlled Voltage Manipulation over Multi-core Frequencies *Pengfei Qiu, Yongqiang Lyu, Dongsheng Wang (Research Institute of Information Technology & BNRist, Tsinghua University, Beijing, China),Gang Qu (University of Maryland, College Park)*	MemGuard: Defending against Black-Box Membership Inference Attacks via Adversarial Examples *Jinyuan Jia (Duke University),Ahmed Salem (CISPA Helmholtz Center for Information Security),Michael Backes (CISPA Helmholtz Center for Information Security),Yang Zhang (CISPA Helmholtz Center for Information Security),Neil Zhenqiang Gong (Duke University)*	LevioSA: Lightweight Secure Arithmetic Computation *Carmit Hazay (Bar-Ilan University),Yuval Ishai (Technion),Antonio Marcedone (Cornell-Tech),Muthu Venkitasubramaniam (University of Rochester)*	Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference *Hao Chen (Microsoft Research),Wei Dai (Microsoft Research),Miran Kim (University of Texas, Health Science Center at Houston),Yongsoo Song (Microsoft Research)*	Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet *Matthew Luckie (University of Waikato),Robert Beverly (Naval Postgraduate School),Ryan Koga (CAIDA / UC San Diego),Ken Keys (CAIDA / UC San Diego),Joshua Kroll (UC Berkeley School of Information),kc claffy (CAIDA / UC San Diego)*
	Principled Unearthing of TCP Side Channel Vulnerabilities *Yue Cao, Zhongjie Wang, Zhiyun Qian, Chengyu Song, Srikanth Krishnamurthy (University of California, Riverside),Paul Yu (Army Research Laboratory)*	Procedural Noise Adversarial Examples for Black-Box Attacks on Deep Convolutional Networks *Kenneth Co (Imperial College London),Luis Muñoz-González (Imperial College London),Sixte de Maupeou (Imperial College London),Emil C. Lupu (Imperial College London)*	Onion Ring ORAM: Efficient Constant Bandwidth Oblivious RAM from (Leveled) TFHE *Hao Chen (Microsoft Research),Ilaria Chillotti (KU Leuven),Ling Ren (VMware Research)*	Traceback for End-to-End Encrypted Messaging *Nirvan Tyagi (Cornell University),Ian Miers (Cornell Tech, University of Maryland),Thomas Ristenpart (Cornell Tech)*	Security Certification in Payment Card Industry: Testbeds, Measurements, and Recommendations *Sazzadur Rahaman (Virginia Tech), Gang Wang (University of Illinois at Urbana-Champaign), Daphne Yao (Virginia Tech)*
15:30	**Coffee Break**				
16:00	**Session 3A: Fuzzing: Methods and Applications** *Chair: Venkat Venkatakrishnan*	**Session 3B: Blockchain I** *Chair: Andrew Miller*	**Session 3C: Secure Computing II** *Chair: Nick Hopper*	**Session 3D: Formal Analysis I** *Chair: Carl Gunter*	**Session 3E: Privacy II** *Chair: Ilya Mironov*
	Matryoshka: fuzzing deeply nested branches *Peng Chen (ByteDance AI lab),Jianzhong Liu (ShanghaiTech University),Hao Chen (University of California, Davis)*	HyperService: Interoperability and Programmability across Heterogeneous Blockchains *Zhuotao Liu (UIUC & Google),Yangxi Xiang (Beijing University of Posts and Telecommunications),Jian Shi (Case Western Reserve University),Peng Gao (University of California, Berkeley),Haoyu Wang (Beijing University of Posts and Telecommunications),Xusheng Xiao (Case Western Reserve University),Bihan Wen (Nanyang Technological University),Yih-Chun Hu (UIUC)*	Securely Sampling Biased Coins with Applications to Differential Privacy *Jeffrey Champion (Northeastern University),Abhi Shelat (Northeastern University),Jonathan Ullman (Northeastern University)*	A Formal Treatment of Deterministic Wallets *Poulami Das (Technische Universität Darmstadt, Germany),Sebastian Faust (Technische Universität Darmstadt, Germany),Julian Loss (Ruhr-Universität Bochum, Germany)*	Analyzing Subgraph Statistics from Extended Local Views with Decentralized Differential Privacy *Haipei Sun (Qatar Computing Research Institute),Xiaokui Xiao (National University of Singapore),Issa Khalil (Qatar Computing Research Institute (QCRI), HBKU),Yin Yang (College of Science and Engineering, Hamad Bin Khalifa University),Zhan Qin (Zhejiang University),Hui (Wendy) Wang (Stevens Institute of Technology),Ting Yu (Qatar Computing Research Institute)*
	Intriguer: Field-Level Constraint Solving for Hybrid Fuzzing *Mingi Cho (Yonsei University),Seoyoung Kim (Yonsei University),Taekyoung Kwon (Yonsei University)*	MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol *Muhammed F. Esgin (Monash University and Data61, CSIRO),Raymond K. Zhao (Monash University),Ron Steinfeld (Monash University),Joseph K. Liu (Monash University),Dongxi Liu (Data61, CSIRO)*	Stormy: Statistics in Tor by Measuring Securely *Ryan Wails (U.S. Naval Research Laboratory),Aaron Johnson (U.S. Naval Research Laboratory),Daniel Starin (Perspecta Labs),Arkady Yerukhimovich (George Washington University),S. Dov Gordon (George Mason University)*	5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol *Syed Rafiul Hussain (Purdue University),Mitziu Echeverria (The University of Iowa),Imtiaz Karim (Purdue University),Omar Chowdhury (The University of Iowa),Elisa Bertino (Purdue University)*	How to accurately and privately identify anomalies *Hafiz Asif (Rutgers University),Periklis Papakonstantinou (Rutgers University),Jaideep Vaidya (Rutgers University)*
	Learning to Fuzz from Symbolic Execution with Application to Smart Contracts *Jingxuan He (ETH Zurich),Mislav Balunovic (ETH Zurich),Nodar Ambroladze (ETH Zurich),Petar Tsankov (ETH Zurich),Martin Vechev (ETH Zurich)*	Prism: Deconstructing the Blockchain to Approach Physical Limits *Vivek Bagaria (Stanford University),Sreeram Kannan (University of Washington Seattle),David Tse (Stanford University),Giulia Fanti (Carnegie Mellon University),Pramod Viswanath (University of Illinois Urbana-Champaign)*	Efficient Publicly Verifiable 2PC over a Blockchain with Applications to Financially-Secure Computations *Ruiyu Zhu (Indiana University Bloomington),Changchang Ding (Indiana University Bloomington),Yan Huang (Indiana University Bloomington)*	Verified Verifiers for Verifying Elections *Thomas Haines (Norwegian University of Science and Technology),Rajev Gore (The Australian National University),Mukesh Tiwari (The Australian National University)*	Differentially Private Nonparametric Hypothesis Testing *Simon Couch (Reed College),Zeki Kazan (Reed College),Kaiyan Shi (Reed College),Andrew Bray (Reed College),Adam Groce (Reed College)*
18:00	**Poster Session (Monarch)**				
19:30	**Business Meeting (Kings - Balmoral)**				

WEDNESDAY

7:30 — **Registration & Breakfast**

	Kings - Balmoral	Kings - Sandringham	Windsor	Blenheim	Buckingham
9:15	**Session 4A: Side Channels II** *Chair: Yinqian Zhang*	**Session 4B: Blockchain II** *Chair: Aggelos Kiayias*	**Session 4C: Secure Computing III** *Chair: Jonathan Katz*	**Session 4D: Formal Analysis II** *Chair: Ninghui Li*	**Session 4E: Privacy III** *Chair: Yang Zhang*
	ZombieLoad: Cross-Privilege-Boundary Data Sampling *Michael Schwarz,Moritz Lipp (Graz University of Technology),Ahmad Moghimi (Worcester Polytechnic Institute),Jo Van Bulck (imec-DistriNet, KU Leuven),Julian Stecklina,Thomas Prescher (Cyberus Technology),Daniel Gruss (Graz University of Technology)*	Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks *Christoph Egger (Friedrich-Alexander-Universität Erlangen-Nürnberg),Pedro Moreno-Sanchez (TU Wien),Matteo Maffei (TU Wien)*	A High-Assurance Evaluator for Machine-Checked Secure Multiparty Computation *Vitor Pereira (INESC TEC & DCC FC Universidade do Porto),Karim Eldefrawy (SRI International)*	Exploiting Symmetries when Proving Equivalence Properties for Security Protocols *Vincent Cheval (INRIA Nancy - Grand Est),Steve Kremer (INRIA Nancy - Grand Est),Itsaka Rakotonirina (INRIA Nancy - Grand Est)*	Five Years of the Right to be Forgotten *Kurt Thomas, Theo Bertram, Elie Bursztein, Stephanie Caro, Hubert Chao, Rutledge Chin Feman, Peter Fleischer, Albin Gustafsson, Jess Hemerly, Chris Hibbert, Luca Invernizzi, Lanah Kammourieh Donnelly, Jason Ketover, Jay Laefer, Paul Nicholas, Yuan Niu, Harjinder Obhi, David Price, Andrew Strait, Al Verney (Google)*
	Fallout: Leaking Data on Meltdown-resistant CPUs *Claudio Canella (Graz University of Technology),Daniel Genkin (University of Michigan),Lukas Giner, Daniel Gruss, Moritz Lipp (Graz University of Technology),Marina Minkin (University of Michigan),Daniel Moghimi (Worcester Polytechnic Institute),Frank Piessens (KU Leuven),Michael Schwarz (Graz University of Technology),Berk Sunar (Worcester Polytechnic Institute),Jo Van Bulck (KU Leuven),Yuval Yarom (University of Adelaide and Data61)*	Erlay: Efficient Transaction Relay for Bitcoin *Gleb Naumenko (University of British Columbia),Gregory Maxwell (Independent),Pieter Wuille (Blockstream),Alexandra (Sasha) Fedorova (University of British Columbia),Ivan Beschastnikh (University of British Columbia)*	Practical Fully Secure Three-Party Computation via Sublinear Distributed ZK Proofs *Ariel Nof (Bar-Ilan University),Yuval Ishai (Technion and UCLA),Elette Boyle (IDC Herzliya),Niv Gilboa (BGU)*	Are These Pairing Elements Correct? Automated Verification and Applications *Susan Hohenberger (Johns Hopkins University),Satyanarayana Vusirikala (University of Texas at Austin)*	(Un)informed Consent: Studying GDPR Consent Notices in the Field *Christine Utz (Ruhr-Universität Bochum),Martin Degeling (Ruhr-Universität Bochum),Sascha Fahl (Ruhr-Universität Bochum),Florian Schaub (University of Michigan),Thorsten Holz (Ruhr-Universität Bochum)*
	SMoTherSpectre: exploiting speculative execution through port contention *Atri Bhattacharyya (EPFL),Alexandra Sandulescu (IBM Zurich),Matthias Neugschwandtner (IBM Zurich),Alessandro Sorniotti (IBM Zurich),Babak Falsafi (EPFL),Mathias Payer (EPFL),Anil Kurmus (IBM Zurich)*	Power Adjusting and Bribery Racing: Novel Mining Attacks in the Bitcoin System *Shang Gao (The Hong Kong Polytechnic University),Zecheng Li (The Hong Kong Polytechnic University),Zhe Peng (The Hong Kong Polytechnic University),Bin Xiao (The Hong Kong Polytechnic University)*	HoneyBadgerMPC and AsynchroMix: Practical Asynchronous MPC and its Application to Anonymous Communication *Donghang Lu (Purdue University),Thomas Yurek (UIUC),Samarth Kulshreshtha (UIUC),Rahul Govind (UIUC),Aniket Kate (Purdue University),Andrew Miller (UIUC)*	Post-Collusion Security and Distance Bounding *Sjouke Mauw (SnT/CSC, University of Luxembourg),Zach Smith (CSC, University of Luxembourg),Jorge Toro-Pozo (CSC, University of Luxembourg),Rolando Trujillo-Rasua (School of Information Technology, Deakin University)*	Moving Beyond Set-It-And-Forget-It Privacy Settings on Social Media *Mainack Mondal (Cornell University / University of Chicago),Günce Su Yılmaz (University of Chicago),Noah Hirsch (University of Chicago),Mohammad Taha Khan (University of Illinois at Chicago),Michael Tang (University of Chicago),Christopher Tran (University of Illinois at Chicago),Chris Kanich (University of Illinois at Chicago),Blase Ur (University of Chicago),Elena Zheleva (University of Illinois at Chicago)*

10:30 — **Coffee Break**

11:00	**Session 5A: Software Security** *Chair: Hao Chen*	**Session 5B: Protocols** *Chair: Carmit Hazay*	**Session 5C: Cloud Security II** *Chair: Kun Sun*	**Session 5D: SDN Security** *Chair: Seungwon Shin*	**Session 5E: Fingerprinting** *Chair: Nils Tippenhauer*
	Binary Control-Flow Trimming *Masoud Ghaffarinia (University of Texas at Dallas),Kevin Hamlen (University of Texas at Dallas)*	Flexible Byzantine Fault Tolerance *Dahlia Malkhi (VMware Research),Kartik Nayak (VMware Research),Ling Ren (VMware Research)*	Houdini's Escape: Breaking the Resource Rein of Linux Control Groups *Xing Gao (University of Memphis),Zhongshu Gu (IBM Research),Zhengfa Li (Independent Researcher),Hani Jamjoom (IBM Research),Cong Wang (Old Dominion University)*	An In-depth Look Into SDN Topology Discovery Mechanisms: Novel Attacks and Practical Countermeasures *Eduard Marin (University of Birmingham),Nicola Bucciol (University of Padua),Mauro Conti (University of Padua)*	Triplet Fingerprinting: More Practical and Portable Website Fingerprinting with N-shot Learning *Payap Sirinam (Navaminda Kasatriyadhiraj Royal Air Force Academy),Nate Matthews, Mohammad Saidur Rahman, Matthew Wright (Rochester Institute of Technology)*
	Program-mandering: Quantitative Privilege Separation *Shen Liu, Dongrui Zeng, Yongzhe Huang, Frank Capobianco (The Pennsylvania State University, University Park),Stephen McCamant (University of Minnesota, Twin Cities),Trent Jaeger, Gang Tan (The Pennsylvania State University, University Park)*	Distributed Vector-OLE: Improved Constructions and Implementation *Adrià Gascón (The Alan Turing Institute / University of Warwick),Mariana Raykova (Google),Leonie Reichert (Humboldt-Universität zu Berlin),Phillipp Schoppmann (Humboldt-Universität zu Berlin)*	Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation *Robert Buhren (Technische Universität Berlin),Christian Werling (Hasso Plattner Institute, Potsdam),Jean-Pierre Seifert(Technische Universität Berlin)*	Proof-Carrying Network Code *Christian Skalka, John Ring, David Darais (University of Vermont),Minseok Kwon, Sahil Gupta, Kyle Diller (Rochester Institute of Technology), Steffen Smolka, Nate Foster (Cornell University)*	DeMiCPU: Device Fingerprinting with Magnetic Signals Radiated by CPU *Yushi Cheng (Zhejiang University),Xiaoyu Ji (Zhejiang University),Juchuan Zhang (Zhejiang University),Wenyuan Xu (Zhejiang University),Yi-Chao Chen (University of Texas at Austin)*

12:00 — **Lunch Break (Monarch)**

13:30	**Session 6A: Biometrics Security** *Chair: Kehuan Zhang*	**Session 6B: ML Security II** *Chair: Neil Gong*	**Session 6C: Secure Computing VI** *Chair: Mike Rosulek*	**Session 6D: Cyber Threat** *Chair: Ting Yu*	**Session 6E: Passwords and Accounts** *Chair: Blase Ur*
	Multisketches: Practical Secure Sketches Using Off-the-Shelf Biometric Matching Algorithms *Rahul Chatterjee (Cornell University),M. Sadegh Riazi (UCSD),Tanmoy Chowdhury (GMU),Emanuela Marasco (GMU),Farinaz Koushanfar (UCSD),Ari Juels (Jacobs Institute, Cornell Tech)*	QUOTIENT: Two-Party Secure Neural Network Training and Prediction *Adria Gascon (The Alan Turing Institute),Ali Shahin Shamsabadi (Queen Mary University London),Nitin Agrawal (University of Oxford),Matthew Kusner (University of Oxford, The Alan Turing Institute)*	PIEs: Public Incompressible Encodings for Decentralized Storage *Ethan Cecchetti (Cornell University),Benjamin Fisch (Stanford University),Ian Miers (Cornell Tech),Ari Juels (Jacobs Institute, Cornell Tech)*	Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise *Fucheng Liu, Yu Wen, Dongxue Zhang, Xihe Jiang (Chinese Academy of Science),Xinyu Xing (The Pennsylvania State University),Dan Meng (Chinese Academy of Science)*	How to (not) share a password: Privacy preserving protocols for finding heavy hitters with adversarial behavior *Moni Naor (Weizmann Institue),Benny Pinkas (Bar Ilan University),Eyal Ronen (Tel Aviv University, KU Leuven)*
	28 Blinks Later: Tackling Practical Challenges of Eye Movement Biometrics *Simon Eberz (University of Oxford),Giulio Lovisotto (University of Oxford),Kasper Rasmussen (University of Oxford),Vincent Lenders (Armasuisse),Ivan Martinovic (University of Oxford)*	Quantitative Verification of Neural Networks and Its Security Applications *Teodora Baluta (National University of Singapore),Shiqi Shen (National University of Singapore),Shweta Shinde (University of California, Berkeley),Kuldeep S. Meel (National University of Singapore),Prateek Saxena (National University of Singapore)*	Probabilistic Data Structures in Adversarial Environments *David Clayton (University of Florida),Christopher Patton (University of Florida),Thomas Shrimpton (University of Florida)*	POIROT: Aligning Attack Behavior with Kernel Audit Records for Cyber Threat Hunting *Sadegh M. Milajerdi (UIC),Birhanu Eshete (University of Michigan-Dearborn),Rigel Gjomemo (UIC),V.N. Venkatakrishnan (UIC)*	Protocols for Checking Compromised Credentials *Lucy Li (Cornell University),Bijeeta Pal (Cornell University),Junade Ali (Cloudflare Inc.),Nick Sullivan (Cloudflare Inc.),Rahul Chatterjee (Cornell University),Thomas Ristenpart (Cornell Tech)*
	Velody: Nonlinear Vibration Challenge-Response for Resilient User Authentication *Jingjie Li (University of Wisconsin-Madison),Younghyun Kim (University of Wisconsin-Madison),Kassem Fawaz (University of Wisconsin-Madison)*	ABS: Scanning Neural Networks for Back-doors by Artificial Brain Stimulation *Yingqi Liu (Purdue University),Wen-Chuan Lee (Purdue University),Guanhong Tao (Purdue University),Shiqing Ma (Purdue University),Yousra Aafer (Purdue University),Xiangyu Zhang (Purdue University)*	Transparency Logs via Append-only Authenticated Dictionaries *Alin Tomescu (MIT),Vivek Bhupatiraju (Lexington High School),Dimitrios Papadopoulos (Hong Kong University of Science and Technology),Charalampos Papamanthou (University of Maryland),Nikos Triandopoulos (Stevens Institute of Technology),Srinivas Devadas (MIT)*	Effective and Light-Weight Deobfuscation and Semantic-Aware Attack Detection for PowerShell Scripts *Zhenyuan LI (Zhejiang University),Qi Alfred Chen (University of California, Irvine),Chunlin Xiong (Zhejiang University),Yan Chen (Northwestern University),Tiantian Zhu (Zhejiang University of Technology),Hai Yang (MagicShield Inc)*	User Account Access Graphs *Sven Hammann (ETH Zurich),Sasa Radomirovic (University of Dundee),Ralf Sasse (ETH Zurich),David Basin (ETH Zurich)*
	The Catcher in the Field: A Fieldprint based Spoofing Detection for Text-Independent Speaker Verification *Chen Yan (Zhejiang University),Yan Long (Zhejiang University),Xiaoyu Ji (Zhejiang University),Wenyuan Xu (Zhejiang University)*	Lifelong Anomaly Detection Through Unlearning *Min Du (University of California Berkeley),Zhi Chen (University of California Berkeley),Chang Liu (Citadel Securities),Rajvardhan Oak (University of California Berkeley),Dawn Song (University of California Berkeley)*	Make Some ROOM for the Zeros: Data Sparsity in Secure Distributed Machine Learning *Phillipp Schoppmann (Humboldt-Universität zu Berlin),Adrià Gascón (The Alan Turing Institute, University of Warwick),Mariana Raykova (Google),Benny Pinkas (Bar Ilan University)*	MalMax: Multi-Aspect Execution for Automated Dynamic Web Server Malware Analysis *Abbas Naderi-Afooshteh (University of Virginia),Yonghwi Kwon (University of Virginia),Jack Davidson (University of Virginia),Anh Nguyen-Tuong (University of Virginia),Ali Razmjoo-Qalaei,Mohammad-Reza Zamiri-Gourabi (ZDResearch)*	Detecting Fake Accounts in Online Social Networks at the Time of Registrations *Dong Yuan (Tsinghua University),Yuanli Miao (Tsinghua University),Neil Zhenqiang Gong (Duke University),Zheng Yang(Tsinghua University),Qi Li (Tsinghua University),Dawn Song (UC Berkeley),Qian Wang (Wuhan University),Xiao Liang (Tencent)*

15:30 — **Coffee Break**

16:00	**Session 7A: Internet of Things** *Chair: Kangjie Lu*	**Session 7B: Blockchain III** *Chair: Danfeng Yao*	**Session 7C: Secure Computing V** *Chair: XiaoFeng Wang*	**Session 7D: Formal Analysis III** *Chair: Matteo Maffei*	**Session 7E: Privacy-Preserving Techniques** *Chair: Jonathan Katz*
	Charting the Attack Surface of Trigger-Action IoT Platforms *Qi Wang, Pubali Datta (University of Illinois at Urbana-Champaign),Wei Yang (The University of Texas at Dallas),Si Liu, Carl Gunter, Adam Bates (University of Illinois at Urbana-Champaign)*	Balance: Dynamic Adjustment of Cryptocurrency Deposits *Dominik Harz (Imperial College London),Lewis Gudgeon (Imperial College London),Arthur Gervais (Imperial College London),William J. Knottenbelt (Imperial College London)*	Efficient MPC via Program Analysis: A Framework for Efficient Optimal Mixing *Muhammad Ishaq (University of Edinburgh),Ana Milanova (Rensselaer Polytechnic Institute),Vassilis Zikas (University of Edinburgh)*	Signed Cryptographic Program Verification with Typed CryptoLine *Yu-Fu Fu (Academia Sinica), Jiaxiang Liu, Xiaomu Shi (Academia Sinica & Shenzhen University), Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang (Academia Sinica)*	SEEMless: Secure End-to-End Encrypted Messaging with less Trust *Melissa Chase (Microsoft Research),Apoorvaa Deshpande (Brown University),Esha Ghosh (Microsoft Research),Harjasleen Malvai (Cornell University)*
	Peeves: Physical Event Verification in Smart Homes *Simon Birnbach (University of Oxford),Simon Eberz (University of Oxford),Ivan Martinovic (University of Oxford)*	TokenScope: Automatically Detecting Inconsistent Behaviors of Cryptocurrency Tokens in Ethereum *Ting Chen,Yufei Zhang,Zihao Li (University of Electronic Science and Technology of China),Xiapu Luo (The Hong Kong Polytechnic University),Ting Wang (Lehigh University),Rong Cao,Xiuzhuo Xiao,Xiaosong Zhang (University of Electronic Science and Technology of China)*	Two-Thirds Honest-Majority MPC for Malicious Adversaries at Almost the Cost of Semi-Honest *Jun Furukawa (NEC Israel Research Center),Yehuda Lindell (Bar-Ilan University and Unbound Tech)*	Machine-Checked Proofs for Cryptographic Standards *José Bacelar Almeida (Universidade do Minho & INESC-TEC),Cécile Baritel-Ruet (Université Côte d'Azur & Inria Sophia-Antipolis),Manuel Barbosa (Universidade do Porto & INESC-TEC),Gilles Barthe (MPI-SP & IMDEA Software Institute),François Dupressoir (University of Surrey & University of Bristol),Benjamin Grégoire (Inria Sophia-Antipolis),Vincent Laporte (Inria),Tiago Oliveira (Universidade do Porto & INESC-TEC & FCUP),Alley Stoughton (Boston University),Pierre-Yves Strub (École Polytechnique)*	PrivDPI: Privacy-Preserving Encrypted Traffic Inspection with Reusable Obfuscated Rules *Jianting Ning (Fujian Normal University & National University of Singapore),Geong Sen Poh (Trustwave & NUS-Singtel Cyber Security Lab),Jia-Ch'ng Loh (NUS-Singtel Cyber Security Lab),Jason Chia (NUS-Singtel Cyber Security Lab),Ee-Chien Chang (National University of Singapore)*
	Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps *Chaoshun Zuo (Ohio State University),Haohuang Wen (Ohio State University),Zhiqiang Lin (Ohio State University),Yinqian Zhang (Ohio State University)*	Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware *Iddo Bentov (Cornell Tech),Ari Juels (Cornell Tech),Fan Zhang (Cornell Tech),Yan Ji (Cornell Tech),Phil Daian (Cornell Tech),Lorenz Breindenbach (ETH Zurich)*	Fast Actively Secure Five-Party Computation with Security Beyond Abort *Megha Byali (Indian Institute of Science, Bangalore),Carmit Hazay (Bar-Ilan University, Israel),Arpita Patra, Swati Singla (Indian Institute of Science, Bangalore)*	VeriSketch: Synthesizing Secure Hardware Designs with Timing-Sensitive Information Flow Properties *Armaiti Ardeshiricham (UCSD),Yoshiki Takashima (UCSD),Sicun Gao (UCSD),Ryan Kastner (UCSD)*	Updatable Anonymous Credentials and Applications to Incentive Systems *Johannes Blömer (Paderborn University),Jan Bobolz (Paderborn University),Denis Diemert (Paderborn University),Fabian Eidens (Paderborn University)*

17:35 — **Panel Discussion: Scaling the Academic Security Community (Kings - Sandringham)**

19:00 — **Banquet (Monarch)**

THURSDAY

7:30 — **Registration & Breakfast**

9:15 — **Keynote: N. Asokan - Hardware-assisted Trusted Execution Environments — Look Back, Look Ahead (Kings)**

10:30 — **Coffee Break**

11:00

Session 8A: Attacks II
Chair: Chao Zhang

Gollum: Modular and Greybox Exploit Generation for Heap Overflows in Interpreters
Sean Heelan (University of Oxford),Daniel Kroening (University of Oxford),Tom Melham (University of Oxford)

SLAKE: Facilitating Slab Manipulation for Exploiting Vulnerabilities in the Linux Kernel
Yueqi Chen (Pennsylvania State University),Xinyu Xing (Pennsylvania State University)

Session 8B: TEE I
Chair: Yuval Yarom

SecTEE: A Software-based Approach to Secure Enclave Architecture Using TEE
Shijun Zhao (Chinese Academy of Sciences),Qianying Zhang (Capital Normal University Information Engineering College),Qin Yu,Wei Feng,Dengguo Feng (Chinese Academy of Sciences)

A Tale of Two Worlds: Assessing the Vulnerability of Enclave Shielding Runtimes
Jo Van Bulck (imec-DistriNet, KU Leuven, Belgium),David Oswald (School of Computer Science, University of Birmingham, UK),Eduard Marin (School of Computer Science, University of Birmingham, UK),Abdulla Aldoseri (School of Computer Science, University of Birmingham, UK),Flavio D. Garcia (School of Computer Science, University of Birmingham, UK),Frank Piessens (imec-DistriNet, KU Leuven, Belgium)

Session 8C: Blockchain VI
Chair: XiaoFeng Wang

zkay: Specifying and Enforcing Data Privacy in Smart Contracts
Samuel Steffen (ETH Zürich),Benjamin Bichsel (ETH Zürich),Mario Gersbach (ETH Zürich),Noa Melchior (ETH Zürich),Petar Tsankov (ETH Zürich),Martin Vechev (ETH Zürich)

Privacy Aspects and Subliminal Channels in Zcash
Alex Biryukov (University of Luxembourg),Daniel Feher (University of Luxembourg),Giuseppe Vitto (University of Luxembourg)

Session 8D: Language Security
Chair: Johannes Kinder

Where Does It Go? Refining Indirect-Call Targets with Multi-Layer Type Analysis
Kangjie Lu (University of Minnesota), Hong Hu (GeorgiaTech)

Different is Good: Detecting the Use of Uninitialized Variables through Differential Replay
Mengchen Cao (Orion Security Lab, Alibaba Group),Xiantong Hou (Orion Security Lab, Alibaba Group),Tao Wang (Orion Security Lab, Alibaba Group),Hunter Qu (Orion Security Lab, Alibaba Group),Yajin Zhou (Zhejiang University),Xiaolong Bai (Orion Security Lab, Alibaba Group),Fuwei Wang (Orion Security Lab, Alibaba Group)

Session 8E: Web Security
Chair: Giovanni Vigna

HideNoSeek: Camouflaging Malicious JavaScript in Benign ASTs
Aurore Fass (CISPA Helmholtz Center for Information Security),Michael Backes (CISPA Helmholtz Center for Information Security),Ben Stock (CISPA Helmholtz Center for Information Security)

Your Cache Has Fallen: Cache-Poisoned Denial-of-Service Attack
Hoai Viet Nguyen (Cologne University of Applied Sciences),Luigi Lo Iacono (Cologne University of Applied Sciences),Hannes Federrath (University of Hamburg)

12:00 — **Lunch Break (Monarch)**

13:30

Session 9A: User Study
Chair: Kassem Fawaz

"I don't see why I would ever want to use it": Analyzing the Usability of Popular Smartphone Password Managers
Sunyoung Seiler-Hwang (University of Mannheim),Patricia Arias-Cabarcos (University of Mannheim),Andrés Marín (University Carlos III of Madrid),Florina Almenares (University Carlos III of Madrid),Daniel Díaz-Sánchez (University Carlos III of Madrid),Christian Becker (University of Mannheim)

Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues
Faris Bugra Kokulu (Arizona State University),Ananta Soneji (Arizona State University),Tiffany Bao (Arizona State University),Yan Shoshitaishvili (Arizona State University),Ziming Zhao (Rochester Institute of Technology),Adam Doupé (Arizona State University),Gail-Joon Ahn (Arizona State University and Samsung Research)

A Usability Evaluation of Let's Encrypt and Certbot - Usable Security Done Right?
Christian Tiefenau (University of Bonn),Emanuel von Zezschwitz (University of Bonn, Fraunhofer FKIE),Maximilian Häring (Fraunhofer FKIE),Katharina Krombholz (CISPA Helmholtz Center for Information Security),Matthew Smith (University of Bonn, Fraunhofer FKIE)

Session 9B: ML Security III
Chair: Esfandiar Mohammadi

Seeing isn't Believing: Towards More Robust Adversarial Attack Against Real World Object Detectors
Yue Zhao,Hong Zhu,Ruigang Liang,Qintao Shen (Chinese Academy of Sciences,University of Chinese Academy of Sciences),Shengzhi Zhang (Metropolitan College, Boston University),Kai Chen (Chinese Academy of Sciences,University of Chinese Academy of Sciences)

AdVersarial: Perceptual Ad Blocking meets Adversarial Machine Learning
Florian Tramèr (Stanford University),Pascal Dupré (CISPA),Gili Rusak (Stanford),Giancarlo Pellegrino (Stanford University, CISPA),Dan Boneh (Stanford University)

Attacking Graph-based Classification via Manipulating the Graph Structure
Binghui Wang (Duke University),Neil Zhenqiang Gong (Duke University)

Latent Backdoor Attacks on Deep Neural Networks
Yuanshun Yao (University of Chicago),Huiying Li (University of Chicago),Haitao Zheng (University of Chicago),Ben Y. Zhao (University of Chicago)

Session 9C: Zero-Knowledge Proofs
Chair: Daniel Genkin

Succinct Arguments for Bilinear Group Arithmetic: Practical Structure-Preserving Cryptography
Russell W. F. Lai (Friedrich-Alexander University Erlangen-Nuremberg),Giulio Malavolta (Carnegie Mellon University),Viktoria Ronge (Friedrich-Alexander University Erlangen-Nuremberg)

LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs
Matteo Campanelli (IMDEA Software Institute, Madrid, Spain),Dario Fiore (IMDEA Software Institute, Madrid, Spain),Anaïs Querol (IMDEA Software Institute, Madrid, and Universidad Politecnica de Madrid, Spain)

Efficient Zero-Knowledge Arguments in the Discrete Log Setting, Revisited
Michael Klooß (Karlsruhe Institute of Technology),Max Hoffmann (Ruhr University Bochum),Andy Rupp (Karlsruhe Institute of Technology)

Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings
Mary Maller (University College London),Sean Bowe (Zcash),Markulf Kohlweiss (University of Edinburgh, IOHK),Sarah Meiklejohn (University College London)

Session 9D: Signatures
Chair: Dominique Schröder

The SPHINCS+ signature framework
Andreas Hülsing (TU Eindhoven),Peter Schwabe (RU Nijmegen),Joost Rijneveld (RU Nijmegen),Stefan Kölbl (Cybercrypt),Daniel J Bernstein (University of Illinois at Chicago and Ruhr University Bochum),Ruben Niederhagen (SIT Fraunhofer)

GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures, Revisited
Gilles Barthe (MPI-SP and IMDEA Software Institute),Sonia Belaid (CryptoExperts),Thomas Espitau (Sorbonne Université),Pierre-Alain Fouque (Univ Rennes),Mélissa Ross (ENS and Thalès),Mehdi Tibouchi (NTT Corporation)

Seems Legit: Automated Analysis of Subtle Attacks on Protocols that use Signatures
Dennis Jackson (University of Oxford),Katriel Cohn-Gordon (Facebook),Cas Cremers (CISPA Helmholtz Center for Information Security),Ralf Sasse (ETH Zürich)

Membership Privacy for Fully Dynamic Group Signatures
Michael Backes (CISPA Helmholtz Center for Information Security),Lucjan Hanzlik (CISPA Helmholtz Center for Information Security, Stanford University),Jonas Schneider-Bensch (CISPA Helmholtz Center for Information Security)

Session 9E: Web Censorship and Auditing
Chair: Rob Jansen

Geneva: Evolving Censorship Evasion Strategies
Kevin Bock (University of Maryland),George Hughey (University of Maryland),Xiao Qiang (UC Berkeley),Dave Levin (University of Maryland)

Conjure: Summoning Proxies from Unused Address Space
Sergey Frolov (University of Colorado Boulder),Jack Wampler (University of Colorado Boulder),Sze Chuen Tan (UIUC),J. Alex Halderman (University of Michigan),Nikita Borisov (UIUC),Eric Wustrow (University of Colorado Boulder)

You Shall Not Join: A Measurement Study of Cryptocurrency Peer-to-Peer Bootstrapping Techniques
Angelique Faye Loe (Royal Holloway, University of London),Elizabeth Quaglia (Royal Holloway, University of London)

SAMPL: Scalable Auditability of Monitoring Processes using Public Ledgers
Roopa Vishwanathan (New Mexico State University),Gaurav Panwar (New Mexico State University),Satyajayant Misra (New Mexico State University),Austin Bos (New Mexico State University)

15:30 — **Coffee Break**

16:00

Session 10A: Cyberphysical Security
Chair: Soteris Demetriou

Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving
Yulong Cao (University of Michigan),Chaowei Xiao (University of Michigan),Benjamin Cyr (University of Michigan),Yimeng Zhou (University of Michigan),Won Park (University of Michigan),Sara Rampazzi (University of Michigan),Qi Alfred Chen (University of California, Irvine),Kevin Fu (University of Michigan),Z. Morley Mao (University of Michigan)

LibreCAN: Automated CAN Message Translator
Mert D. Pesé (University of Michigan, Ann Arbor),Troy Stacer (University of Michigan, Ann Arbor),C. Andrés Campos (University of Michigan, Ann Arbor),Eric Newberry (University of Michigan, Ann Arbor),Dongyao Chen (University of Michigan, Ann Arbor),Kang G. Shin (University of Michigan, Ann Arbor)

Trick or Heat? Manipulating Critical Temperature-Based Control Systems using Rectification attacks
Yazhou Tu (University of Louisiana at Lafayette),Sara Rampazzi (University of Michigan),Bin Hao (University of Louisiana at Lafayette),Angel Rodriguez (University of Michigan),Kevin Fu (University of Michigan),Xiali Hei (University of Louisiana at Lafayette)

Session 10B: TEE II
Chair: Sven Bugiel

OPERA: Open Remote Attestation for Intel's Secure Enclaves
Guoxing Chen (The Ohio State University),Yinqian Zhang (The Ohio State University),Ten-Hwang Lai (The Ohio State University)

Towards Memory Safe Enclave Programming with Rust-SGX
Huibo Wang (University of Texas at Dallas),Pei Wang (Baidu X-Lab),Yu Ding (Baidu X-Lab),Mingshen Sun (Baidu X-Lab),Yiming Jing (Baidu X-Lab),Ran Duan (Baidu X-Lab),Long Li (Baidu X-Lab),Yulong Zhang (Baidu X-Lab),Tao Wei (Baidu X-Lab),Zhiqiang Lin (Ohio State University)

LightBox: Full-stack Protected Stateful Middlebox at Lightning Speed
Huayi DUAN (City University of Hong Kong),Cong Wang (City University of Hong Kong),Xingliang Yuan (Monash University),Yajin Zhou (Zhejiang University),Qian Wang (Wuhan University),Kui Ren (Zhejiang University)

Session 10C: Secret Sharing
Chair: Lorenzo Cavallaro

CHURP: Dynamic-Committee Proactive Secret Sharing
Sai Krishna Deepak Maram (Cornell Tech),Fan Zhang (Cornell Tech),Lun Wang (UC Berkeley),Andrew Low (UC Berkeley),Yupeng Zhang (UC Berkeley and Texas A&M),Ari Juels (Jacobs Institute, Cornell Tech),Dawn Song (UC Berkeley)

Efficient Verifiable Secret Sharing with Share Recovery in BFT Protocols
Soumya Basu (Cornell University, IC3, VMWare Research),Alin Tomescu (MIT, VMWare Research),Ittai Abraham (VMware Research),Dahlia Malkhi (VMWare),Mike Reiter (UNC, VMWare Research),Emin Gün Sirer (Cornell, IC3)

Two-party Private Set Intersection with an Untrusted Third Party.
Phi Hung Le (George Mason University),Samuel Ranellucci (University of Maryland, George Mason University),S. Dov Gordon (George Mason University)

Session 10D: Mobile Security
Chair: Adam Doupé

DeepIntent: Deep Icon-Behavior Learning for Detecting Intention-Behavior Discrepancy in Mobile Apps
Shengqu Xi (Nanjing University),Shao Yang (Case Western Reserve University),Xusheng Xiao (Case Western Reserve University),Yuan Yao (Nanjing University),Yayuan Xiong (Nanjing University),Fengyuan Xu (National Key Lab for Novel Software Technology, Nanjing University),Haoyu Wang (Beijing University of Posts and Telecommunications),Peng Gao (University of California, Berkeley),Zhuotao Liu (University of Illinois at Urbana-Champaign),Feng Xu (Nanjing University),Jian Lu (Nanjing University)

The Art and Craft of Fraudulent App Promotion in Google Play
Mizanur Rahman (Amazon),Nestor Hernandez (FIU),Ruben Recabarren (FIU),Syed Ishtiaque Ahmed (University of Toronto),Bogdan Carbunar (FIU)

CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects
Sazzadur Rahaman (Virginia Tech),Ya Xiao (Virginia Tech),Sharmin Afrose (Virginia Tech),Fahad Shaon (The University of Texas at Dallas),Ke Tian (Virginia Tech),Miles Frantz (Virginia Tech),Danfeng (Daphne) Yao (Virginia Tech),Murat Kantarcioglu (The University of Texas at Dallas)

Session 10E: Certificates
Chair: Tudor Dumitras

Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web
Josh Aas (Let's Encrypt),Richard Barnes (Cisco),Benton Case (Stanford University),Zakir Durumeric (Stanford University),Peter Eckersley (Electronic Frontier Foundation),Alan Flores-López (Stanford University),J. Alex Halderman (University of Michigan),Jacob Hoffman-Andrews (Electronic Frontier Foundation),James Kasten (University of Michigan),Eric Rescorla (Mozilla),Seth Schoen (Electronic Frontier Foundation),Brad Warren (Electronic Frontier Foundation)

You Are Who You Appear to Be: A Longitudinal Study of Domain Impersonation in TLS Certificates
Richard Roberts (University of Maryland),Yaelle Goldschlag (University of Maryland),Rachel Walter (University of Maryland),Taejoong Chung (Rochester Institute of Technology),Alan Mislove (Northeastern University),Dave Levin (University of Maryland)

Certificate Transparency in the Wild: Exploring the Reliability of Monitors
Bingyu Li (Institute of Information Engineering, CAS),Jingqiang Lin (Institute of Information Engineering, CAS),Fengjun Li (The University of Kansas, Lawrence),Qiongxiao Wang (Institute of Information Engineering, CAS),Qi Li (Tsinghua University, China),Jiwu Jing ,Congli Wang (Institute of Information Engineering, CAS)