

2025 IEEE 38th Computer Security Foundations Symposium (CSF 2025)

**Santa Cruz, California, USA
16-20 June 2025**



**IEEE Catalog Number: CFP25037-POD
ISBN: 979-8-3315-1082-4**

**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:	CFP25037-POD
ISBN (Print-On-Demand):	979-8-3315-1082-4
ISBN (Online):	979-8-3315-1081-7
ISSN:	1940-1434

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 38th IEEE Computer Security Foundations Symposium (CSF) **CSF 2025**

Table of Contents

Preface	x
Committees	xi
Program Committee	xii
External Reviewers	xiv

Session 1 - Formal Methods and Cryptography

Cryptographically Assured Information Flow: Assured Remote Execution	1
<i>Scott Dyer (The MITRE Corporation), Christian Femrite (The MITRE Corporation), Joshua Guttman (The MITRE Corporation), Julian Lanson (The MITRE Corporation), and Moses Liskov (The MITRE Corporation)</i>	
Secrecy by typing in the computational model	17
<i>Stéphanie Delaune (Univ. Rennes, CNRS, IRISA, France), Clément Hérourard (Univ. Rennes, CNRS, IRISA, France), and Joseph Lallemand (Univ. Rennes, CNRS, IRISA, France)</i>	
Strands Rocq: Why is a Security Protocol Correct, Mechanically?	33
<i>Matteo Busi (Ca' Foscari University of Venice, Italy), Riccardo Focardi (Ca' Foscari University of Venice, Italy), and Flaminia L. Luccio (Ca' Foscari University of Venice, Italy)</i>	
AGATE: Augmented Global Attested Trusted Execution in the Universal Composability framework	49
<i>Lorenzo Martinico (University of Edinburgh, UK; Input Output, UK) and Markulf Kohlweiss (University of Edinburgh, UK; Input Output, UK)</i>	

Session 2 - Privacy and Quantitative Information Flow

Self-Defense: Optimal QIF Solutions and Application to Website Fingerprinting	65
<i>Andreas Athanasiou (INRIA, École Polytechnique), Konstantinos Chatzikokolakis (National and Kapodistrian University of Athens), and Catuscia Palamidessi (INRIA, École Polytechnique)</i>	
Actual Knowledge Gain as Privacy Loss in Local Privacy Accounting	81
<i>Mingen Pan (Independent Researcher)</i>	
Improving Count-Mean Sketch as the Leading Locally Differentially Private Frequency Estimator for Large Dictionaries	97
<i>Mingen Pan (Independent Researcher)</i>	

Session Types for the Concurrent Composition of Interactive Differential Privacy	113
<i>Victor Sannier (Univ. Lille, CNRS, Inria, Centrale Lille, UMR 9189 CRISTAL, F-59 000, France), Patrick Baillot (Univ. Lille, CNRS, Inria, Centrale Lille, UMR 9189 CRISTAL, F-59 000, France), and Marco Gaboardi (Boston University, USA)</i>	

Session 3 - Cryptographic Constructions

Privacy-preserving server-supported decryption	127
<i>Peeter Laud (Cybernetica AS, Estonia), Alisa Pankova (Cybernetica AS, Estonia), and Jelizaveta Vakarjuk (Cybernetica AS, Estonia and Tallinn University of Technology, Estonia)</i>	
Scalable Private Signaling	143
<i>Sashidhar Jakkamsetti (Bosch Research), Zeyu Liu (Yale University), and Varun Madathil (Yale University)</i>	
Foundations of Multi-Designated Verifier Signature: Comprehensive Formalization and New Constructions in Subset Simulation	159
<i>Keitaro Hashimoto (National Institute of Advanced Industrial Science and Technology (AIST), Japan), Kyosuke Yamashita (Osaka University, Japan and National Institute of Advanced Industrial Science and Technology (AIST), Japan), and Keisuke Hara (National Institute of Advanced Industrial Science and Technology (AIST), Japan and Yokohama National University, Japan)</i>	

Session 4 - Attack Models

Pessimism of the Will, Optimism of the Intellect: Fair Protocols with Malicious but Rational Agents	175
<i>Léonard Brice (Université libre de Bruxelles, Belgium), Jean-François Raskin (Université libre de Bruxelles, Belgium), Mathieu Sassolas (Université libre de Bruxelles, Belgium), Guillaume Scerri (Université Paris-Saclay, ENS Paris-Saclay & CNRS, France), and Marie Van Den Bogaard (Université Gustave Eiffel, CNRS, France)</i>	
On DoS Vulnerability of Regular Expressions, with and without Backreferences	190
<i>Tachio Terauchi (Waseda University, Japan)</i>	
Rethinking Attack Path Management: A New Metric for Choke Points in Attack Graphs	205
<i>Yumeng Zhang (The University of Adelaide, Australia), Max Ward (University of Western Australia, Australia), and Hung Nguyen (The University of Adelaide, Australia)</i>	

Session 5 - IoT and Cyber-Physical Security

Path Privacy and Handovers: Preventing Insider Traceability Attacks During Secure Handovers	220
<i>Bhagya Wimalasiri (University of Sheffield, United Kingdom), Benjamin Dowling (King's College London, United Kingdom), and Rabiah Alnashwan (University of Sheffield, United Kingdom)</i>	

Formal Robustness for Cyber-Physical Systems under Timed Attacks	236
<i>Jian Xiang (University of North Carolina at Charlotte), Simone Tini (University of Insubria), Ruggero Lanotte (University of Insubria), and Massimo Merro (University of Verona)</i>	

Session 6 - Information Flow

Accountability, Involvement, and Mediation for Information Flow	252
<i>Elisavet Kozyri (UiT The Arctic University of Norway), Fred Schneider (Cornell University), and Stephen Chong (Harvard University)</i>	
A graded modal approach to relaxed semantic declassification	268
<i>Vineet Rajani (University of Kent, United Kingdom), Alex Coleman (University of Kent, United Kingdom), and Hrutvik Kanabar (University of Kent, United Kingdom)</i>	
Securing P4 Programs by Information Flow Control	284
<i>Anoud Alshnakat (KTH Royal Institute of Technology), Amir M. Ahmadian (KTH Royal Institute of Technology), Musard Balliu (KTH Royal Institute of Technology), Roberto Guanciale (KTH Royal Institute of Technology), and Mads Dam (KTH Royal Institute of Technology)</i>	

Session 7 - Blockchains and Cryptocurrency

Atomic Transfer Graphs: Secure-by-design Protocols for Heterogeneous Blockchain Ecosystems....	300
<i>Stephan Dübler (MPI-SP), Federico Badaloni (MPI-SP), Pedro Moreno-Sanchez (IMDEA Software Institute, VISA Research, MPI-SP), and Clara Schneidewind (MPI-SP)</i>	
BitMLx: Secure Cross-chain Smart Contracts For Bitcoin-style Cryptocurrencies	316
<i>Federico Badaloni (MPI-SP), Sebastian Holler (MPI-SP), Chrysoula Oikonomou (Aristotle University of Thessaloniki), Pedro Moreno-Sanchez (IMDEA Software Institute, VISA Research, MPI-SP), and Clara Schneidewind (MPI-SP)</i>	
VRaaS: Verifiable Randomness as a Service on Blockchains	331
<i>Jacob Gorman (Supra Research), Lucjan Hanzlik (CISPA Helmholtz Center for Information Security), Aniket Kate (Supra Research / Purdue University), Easwar Vivek Mangipudi (Supra Research), Pratyay Mukherjee (Supra Research), Pratik Sarkar (Supra Research), and Sri AravindaKrishnan Thyagarajan (University of Sydney)</i>	

Session 8 - Protocol Verification

One For All: Formally Verifying Protocols which use Aggregate Signatures	347
<i>Xenia Hofmeier (ETH Zurich, Switzerland), Andrea Raguso (ETH Zurich, Switzerland), Ralf Sasse (ETH Zurich, Switzerland), Dennis Jackson (Mozilla, UK), and David Basin (ETH Zurich, Switzerland)</i>	
Nominal State-Separating Proofs	363
<i>Markus Krabbe Larsen (IT University of Copenhagen) and Carsten Schürmann (IT University of Copenhagen)</i>	

Symbolic Parallel Composition for Multi-language Protocol Verification	378
<i>Faezeh Nasrabadi (CISPA Helmholtz Center for Information Security and Saarland University), Robert Kuennemann (CISPA Helmholtz Center for Information Security), and Hamed Nemati (Department of Computer Science, KTH Royal Institute of Technology)</i>	
Formal Analysis of Random Nonce Misuses in Cryptographic Protocols	394
<i>Gildas Avoine (INSA Rennes, Univ Rennes, CNRS, IRISA, IUF, France), Tristan Claverie (ANSSI, INSA Rennes, IRISA, France), and Stéphanie Delaune (Univ Rennes, CNRS, IRISA, France)</i>	

Session 9 - Machine Learning and Privacy

A Novel Approach to Differential Privacy with Alpha Divergence	410
<i>Yifeng Liu (The University of British Columbia, Vancouver) and Zehua Wang (The University of British Columbia, Vancouver)</i>	
Unveiling the (in)Security of Threshold FHE-based Federated Learning: The Practical Impact of Recent CPAD Attacks	425
<i>Adda Akram Bendoukha (Samovar, Télécom SudParis, Institut Polytechnique de Paris), Renaud Sirdey (Université Paris Saclay, CEA-LIST), Aymen Boudguiga (Université Paris-Saclay, CEA-LIST), and Nesrine Kaaniche (Samovar, Télécom SudParis, Institut Polytechnique de Paris)</i>	

Session 10 - Cryptographic Verification

Zero-Knowledge Proofs from Learning Parity with Noise: Optimization, Verification, and Application	441
<i>Thomas Haines (Australian National University), Johannes Müller (LORIA/INRIA/CNRS), Rafieh Mosaheb (SnT/University of Luxembourg), and Reetika Reetika (Indian Institute of Space Science and Technology)</i>	
Verifiable E-Voting with a Trustless Bulletin Board	457
<i>Daniel Rausch (Institute of Information Security, Germany), Nicolas Huber (University of Stuttgart, Germany), and Ralf Küsters (University of Stuttgart, Germany)</i>	
Dynamic Group Signatures with Verifier-Local Revocation	473
<i>Callum London (University of Surrey), Daniel Gardham (University of Surrey), and Constantin Cătălin Drăgan (University of Surrey)</i>	

Session 11 - Automated Verification

Automated Analysis and Synthesis of Message Authentication Codes	489
<i>Julian Thomas (Friedrich-Alexander-Universität Erlangen-Nürnberg), Stefan Milius (Friedrich-Alexander-Universität Erlangen-Nürnberg), Dominik Paulus (Friedrich-Alexander-Universität Erlangen-Nürnberg), Dominique Schröder (TU Wien), and Lutz Schröder (Friedrich-Alexander-Universität Erlangen-Nürnberg)</i>	

SMT-based Automation for Overwhelming Truth	505
<i>David Baelde (Univ Rennes, CNRS, IRISA, France), Stéphanie Delaune (Univ Rennes, CNRS, IRISA, France), and Stanislas Riou (Univ Rennes, CNRS, IRISA, France)</i>	

Automatic verification of Finite Variant Property beyond convergent equational theories	521
<i>Vincent Cheval (University of Oxford) and Caroline Fontaine (Université Paris-Saclay, CNRS, ENS Paris-Saclay, Laboratoire Méthodes Formelles)</i>	

Session 12 - Information Flow

Nonmalleable Progress Leakage	537
<i>Ethan Cecchetti (University of Wisconsin-Madison)</i>	

Gradual Sensitivity Typing	553
<i>Damián Arquez (University of Chile & IMFD, Chile), Matías Toro (University of Chile & IMFD), and Éric Tanter (University of Chile & IMFD)</i>	

FSLH: Flexible Mechanized Speculative Load Hardening	569
<i>Jonathan Baumann (MPI-SP, Germany and ENS Paris-Saclay, France), Roberto Blanco (MPI-SP, Germany and TU/e, Netherlands), Léon Ducruet (MPI-SP, Germany and ENS Lyon, France), Sebastian Harwig (MPI-SP and Ruhr University Bochum, Germany), and Catalin Hritcu (MPI-SP, Germany)</i>	

An Extension of the Adversarial Threat Model in Quantitative Information Flow	585
<i>Mohammad Amin Zarrabian (Australian National University) and Parastoo Sadeghi (University of New South Wales, Canberra)</i>	

Author Index	601
---------------------------	------------