2026 IEEE 39th Computer Security Foundations Symposium (CSF 2026)

Lisboa, Portugal
26-29 July 2026

IEEE Catalog Number: CFP26037-POD
ISBN: 979-8-3195-1807-1

IEEE Advancing Technology for Humanity

Copyright © 2026, IEEE

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:	CFP26037-POD
ISBN (Print-On-Demand):	979-8-3195-1807-1
ISBN (Online):	979-8-3195-1806-4
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



TABLE OF CONTENTS

Incremental Fingerprinting in an Open World 1
Loes Kruger, Paul Kobialka, Andrea Pferscher, Einar Broch Johnsen, Sebastian Junges, Jurriaan Rot

Tamarin Unchained: Handling User-Defined AC Operators 17
Jannik Dreier, Elise Klein, Steve Kremer

Which attacks are most critical? Risk prioritization via attack tree importance measures 33
Reza Soltani, Milan Lopuhaä-Zwakenberg, Mariëlle Stoelinga

BlindReview: Anonymous and End-to-End Verifiable Peer Review 49
Xavier Bultel, Ashley Fraser, Elizabeth A. Quaglia

Time-Lock Puzzles with Preprocessing: an Instantiation from Average-Case Hardness Assumptions on Graphs and Lattices 65
Răzvan Roşie

Self-Guarding Arbitrary Cryptographic Primitives and 2PC Protocols 81
Daniele Friolo, Andrea Reale, Daniele Venturi

Beyond the Finite Variant Property: Extending Symbolic Diffie-Hellman Group Models 96
Sofia Giampietro, Ralf Sasse, David Basin

Are ideal functionalities really ideal? 112
Myrto Arapinis, Véronique Cortier, Hubert de Groote, Charlie Jacomme, Steve Kremer

Bayesian Advantage of Re-Identification Attack in the Shuffle Model 128
Pengcheng Su, Haibo Cheng, Ping Wang

Formalizing Privacy in Decentralized Identity: A Provably Secure Framework with Minimal Disclosure 143
Yu Zhang, Zongbin Wang

A new measure for dynamic leakage based on quantitative information flow 155
Luigi D. C. Soares, Mário S. Alvim, Natasha Fernandes

Privacy Mechanism Design based on Empirical Distributions 171
Leonhard Grosse, Sara Saeidian, Mikael Skoglund, Tobias J. Oechtering

Optimizing Differential Privacy in Federated Analytics under Known Input Distributions 187
Ferran Alborch, Andreas Athanasiou, Pascal Reisert

Interpreting Differential Privacy in Terms of Disclosure Risk 203
Zeki Kazan, Sagar Sharma, Wanrong Zhang, Bo Jiang, Qiang Yan

A Unified Compositional View of Attack Tree Metrics 221
Benedikt Peterseim, Milan Lopuhaä-Zwakenberg

Mind the Gap Connecting Protocol Representations in Squirrel 236
David Baelde, Stéphanie Delaune, Julia Gabet, Clément Hérouard

Towards Strong Certified Defense with Universal Asymmetric Randomization 252
Hanbin Hong, Ashish Kundu, Ali Payani, Binghui Wang, Yuan Hong

LAP$_2$: Revisiting Laplace DP-SGD for High Dimensions via Majorization Theory 268
Meisam Mohammady, Qin Yang, Nicholas Stout, Ayesha Samreen, Han Wang, Christopher J Quinn Yuan Hong

On the Necessity of Pre-agreed Secrets for Thwarting Last-minute Coercion: Vulnerabilities and Lessons From the Loki E-voting Protocol 284
Jingxin Qiao, Myrto Arapinis, Thomas Zacharias

On the design of Survivable Distributed Passwordless Authentication and Single Sign-On 300
Luca Ferretti, Federico Magnanini, Mauro Andreolini, Mattia Trabucco, Michele Colajanni

Simultaneously Proving Privacy and Verifiability: A ProVerif Framework for Internet Voting 316
Vincent Cheval, Veronique Cortier, Alexandre Debant, Florian Moser

Zero-Knowledge Proof of Progress: Secure Multi-Phase Capture-the-Flag Competitions 332
Salam Khanji, Behzad Abdolmaleki, John Clark, Aryan Pasikhani

DPEI: Privacy Budget Savings for Edge Information Protection in Synthetic Graph Publishing 348
Ruizhong Du, Zizhan Wei, Mingyue Li

CHIP: Efficient Homomorphic Encryption-Based CNN Batch Inference Using Channel-Interleaved Packing with Small Rotation Key Set 364
Huan-Chih Wang, Ja-Ling Wu

Setup Protocols for Sender Anonymity 376
Tian Huang, Jiatai Zhang, Megumi Ando

Revisiting Beimel-Weinreb Weighted Threshold Secret Sharing Schemes 392
Oriol Farràs, Miquel Guiot

Partial Cast Calculus for Gradual Information Security 408
Zechi Shen, Zhiwu Xu, Shengchao Qin, Zhong Ming

NTRU with Hints: Secret Key Recovery under Partial Leakage on NTRU-based Signatures 424
Honglin Shao, Yuejun Liu, Mingyao Shao, Wei Cheng, Yongbin Zhou

Dolev-Yao Information Flow 439
Simon Lund, Sebastian Mödersheim

Cryptographic Choreographies 454
Sebastian Mödersheim, Simon Lund, Alessandro Bruni, Marco Carbone, Rosario Giustolisi

Beyond Blockchain Ballots: UC-Secure Layer-2 Voting and Governance 470
Raghav Bhaskar, Pooya Farshim, Matthias Fitzi, Aggelos Kiayias

Verifying and Monitoring the Lightweight Directory Access Protocol (LDAP) 486
Precious Zemoh Ndzebelai, Robert Künnemann

Composing Hybrid Arguments in Nominal-SSProve 500
Markus Krabbe Larsen, Carsten Schürmann

Beyond Epsilon: A Principled QIF Framework for Local Differential Privacy 514
Ramon G. Gonze, Natasha Fernandes, Hèber H. Arcolezi, Catuscia Palamidessi, Nataliia Bielova

Formal Verification of Probing Security via Conditional Independence 528
Satoshi Kura, Katsuyuki Takashima

A Composable Game-Theoretic Framework for Blockchains 544
Zeta Avarikioti, Georg Fuchsbauer, Pim Keer, Matteo Maffei, Fabian Regen

Interactive Proofs in Higher-Order Logic with Errors and Application to Concrete Cryptography 560
Caroline Fontaine, Adrien Koutsos, Guillaume Scerri, Théo Vignon

Triosecuris: Formally Verified Protection Against Speculative Control-Flow Hijacking 575
Jonathan Baumann, Yonghyun Kim, Yan Farba, Căată̆alin Hriţcu, Julay Leatherman-Brooks

Forking Lemma in EasyCrypt 591
Denis Firsov, Jakub Janků

Information Leakage Envelopes 605
Sara Saeidian, Carlos Pinzón, Catuscia Palamidessi

Computationally Sound Symbolic Cryptography in Lean 620
Stefan Dziembowski, Grzegorz Fabiańnski, Daniele Micciancio, Rafań Stefańnski

Active Cyber Defense Strategy through Multi-Agent Systems Verification 636
Gabriel Ballot, Etienne Borde, Vadim Ma Lvone, Jean Leneutre, Jingxuan Ma