2024 IEEE 37th Computer Security Foundations Symposium (CSF 2024)

Enschede, Netherlands
8-12 July 2024

IEEE Catalog Number:	**CFP24037-POD**
ISBN:	**979-8-3503-6204-6**

Copyright © 2024 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:	CFP24037-POD
ISBN (Print-On-Demand):	979-8-3503-6204-6
ISBN (Online):	979-8-3503-6203-9
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

2024 37th IEEE Computer Security Foundations Symposium (CSF)

CSF 2024

Table of Contents

Preface .... **xi**
Committees .... **xii**

Session 1: Privacy

A Systematic and Formal Study of the Impact of Local Differential Privacy on Fairness: Preliminary Results 1
Karima Makhlouf (Inria Saclay and École Polytechnique (IPP), France), Tamara Stefanovic (Mathematical Institute of the Serbian Academy of Sciences and Arts, Serbia), Héber H. Arcolezi (Inria Centre at the University Grenoble Alpes, France), and Catuscia Palamidessi (Inria Saclay and École Polytechnique (IPP), France)

A Decision Procedure for Alpha-Beta Privacy for a Bounded Number of Transitions 17
Laouen Fernet (Danmarks Tekniske Universitet, Danmark), Sebastian Mödersheim (Danmarks Tekniske Universitet, Danmark), and Luca Viganò (King's College London, United Kingdom)

Epistemic Model Checking for Privacy 33
Fortunat Rajaona (University of Surrey, United Kingdom), Ioana Boureanu (University of Surrey, United Kingdom), Ramaswamy Ramanujam (Institute of Mathematical Sciences Chennai, India), and Steve Wesemeyer (University of Surrey, United Kingdom)

Divide and Funnel: A Scaling Technique for Mix-Networks 49
Debajyoti Das (KU Leuven, Belgium), Sebastian Meiser (University of Lübeck, Germany), Esfandiar Mohammadi (University of Lübeck, Germany), and Aniket Kate (Purdue University, USA; Supra Research, USA)

Session 2: Verification

Deciding branching hyperproperties for real time systems 65
Nabarun Deka (University of Illinois at Urbana-Champaign), Minjian Zhang (University of Illinois at Urbana-Champaign), Rohit Chadha (University of Missouri), and Mahesh Viswanathan (University of Illinois at Urbana-Champaign)

On Separation Logic, Computational Independence, and Pseudorandomness 80
Ugo Dal Lago (University of Bologna, Inria), Davide Davoli (Inria, Université Côte d'Azur), and Bruce M. Kapron (University of Victoria)

Probability from Possibility: Probabilistic Confidentiality for Storage Systems Under Nondeterminism 96
Atalay Ileri (Kansas State University, USA), Nickolai Zeldovich (Massachusetts Institute of Technology, USA), Adam Chlipala (Massachusetts Institute of Technology, USA), and Frans Kaashoek (Massachusetts Institute of Technology, USA)

Brewer-Nash Scrutinised: Mechanised Checking of Policies featuring Write Revocation 112
Alfredo Capozucca (University of Luxembourg), Maximiliano Cristiá (Universidad Nacional de Rosario and CIFASIS, Argentina), Ross Horne (University of Strathclyde, United Kingdom), and Ricardo Katz (CIFASIS CONICET, Argentina)

Session 3: Blockchains and smart contracts

Recent Latest Message Driven GHOST: Balancing Dynamic Availability With Asynchrony Resilience 127
Francesco D'Amato (Ethereum Foundation) and Luca Zanolini (Ethereum Foundation)

Consensus Redux: Distributed Ledgers in the Face of Adversarial Supremacy 143
Christian Badertscher (Input Output, Switzerland), Peter Gaži (Input Output, Slovakia), Aggelos Kiayias (University of Edinburgh and Input Output, United Kingdom), Alexander Russell (University of Connecticut and Input Output, USA), and Vassilis Zikas (Purdue University, USA)

Modeling Mobile Crash in Byzantine Consensus 159
Hans Schmiedel (Monash University), Runchao Han (BabylonChain Inc.), Qiang Tang (The University of Sydney), Ron Steinfeld (Monash University), and Jiangshan Yu (The University of Sydney)

A Maintainable Matrix Commitment Scheme with Constant-Size Public Parameters and Incremental Aggregation 172
Wenhui Qiao (ShanghaiTech University, China) and Liang Feng Zhang (ShanghaiTech University, China)

Session 4: Voting

Is the JCJ Voting System Really Coercion-Resistant? 186
Véronique Cortier (Université de Lorraine, CNRS, Inria - LORIA), Pierrick Gaudry (Université de Lorraine, CNRS, Inria - LORIA), and Quentin Yang (Université de Lorraine, CNRS, Inria - LORIA)

Accountable Bulletin Boards: Definition and Provably Secure Implementation 201
Mike Graf (University of Stuttgart, Germany), Ralf Küsters (University of Stuttgart, Germany), Daniel Rausch (University of Stuttgart, Germany), Simon Egger (University of Stuttgart, Germany), Marvin Bechtold (University of Stuttgart, Germany), and Marcel Flinspach (University of Stuttgart, Germany)

Publicly Auditable Privacy-Preserving Electoral Rolls 217
Prashant Agrawal (Indian Institute of Technology Delhi, India; Ashoka University, India), Mahabir Prasad Jhanwar (Ashoka University, India), Subodh Vishnu Sharma (Indian Institute of Technology Delhi, India), and Subhashis Banerjee (Ashoka University, India)

Session 5: Security Analysis

Bridging the Gap: Automated Analysis of Sancus 233
Matteo Busi (Ca' Foscari University of Venice), Riccardo Focardi (Ca' Foscari University of Venice), and Flaminia Luccio (Ca' Foscari University of Venice)

Wappler: Sound Reachability Analysis for WebAssembly 249
Markus Scherer (TU Wien), Jeppe Fredsgaard Blaabjerg (Aarhus University), Alexander Sjösten (TU Wien), Magdalena Solitro (TU Wien), and Matteo Maffei (TU Wien)

Session 6: Crypto

Computationally Bounded Robust Compilation and Universally Composable Security 265
Robert Künnemann (CISPA Helmholtz Center for Information Security), Marco Patrignani (University of Trento), and Ethan Cecchetti (University of Wisconsin–Madison)

CV2EC: Getting the Best of Both Worlds 279
Bruno Blanchet (Inria, France), Pierre Boutry (Université Côte d'Azur, Inria, France), Christian Doczkal (Max Planck Institute for Security and Privacy, Germany), Benjamin Grégoire (Université Côte d'Azur, Inria, France), and Pierre-Yves Strub (PQShield, France)

On Efficient and Secure Compression Functions for Arithmetization-Oriented Hashing 295
Elena Andreeva (TU Wien), Rishiraj Bhattacharyya (University of Birmingham), Arnab Roy (University of Innsbruck), and Stefano Trevisani (TU Wien)

Inject Less, Recover More: Unlocking the Potential of Document Recovery in Injection Attacks Against SSE 311
Manning Zhang (Delft University of Technology), Zeshun Shi (Delft University of Technology), HuanHuan Chen (Delft University of Technology), and Kaitai Liang (Delft University of Technology)

Session 7: Logics for security

A Probabilistic Logic for Concrete Security 324
David Baelde (Univ Rennes, CNRS, IRISA, France), Caroline Fontaine (Université Paris-Saclay, CNRS, ENS Paris-Saclay, LMF, Gif-sur-Yvette, France), Adrien Koutsos (Inria Paris, France), Guillaume Scerri (Université Paris-Saclay, CNRS, ENS Paris-Saclay, LMF, Gif-sur-Yvette, France), and Théo Vignon (Université Paris-Saclay, CNRS, ENS Paris-Saclay, LMF, Gif-sur-Yvette, France)

Security Properties through the Lens of Modal Logic 340
Matvey Soloviev (KTH Royal Institute of Technology, Sweden), Musard Balliu (KTH Royal Institute of Technology, Sweden), and Roberto Guanciale (KTH Royal Institute of Technology, Sweden)

A Logic of Sattestation 356
Aaron D. Jaggard (U.S. Naval Research Laboratory), Paul Syverson (U.S. Naval Research Laboratory), and Catherine Meadows (U.S. Naval Research Laboratory)

Session 8: Language-based security

ZK-SecreC: A Domain-Specific Language for Zero-Knowledge Proofs 372
Dan Bogdanov (Cybernetica AS, Estonia), Joosep Jääger (Input Output (IOHK), Estonia), Peeter Laud (Cybernetica AS, Estonia), Härmel Nestra (Cybernetica AS, Estonia), Martin Pettai (Cybernetica AS, Estonia), Jaak Randmets (Artificial Labs, Estonia), Raul-Martin Rebane (Cybernetica AS), Ville Sokk (Artificial Labs, Estonia), Kert Tali (Cybernetica AS, Estonia), and Sandhra-Mirella Valdma (Cybernetica AS, Estonia)

Disjunctive Policies for Database-Backed Programs 388
Amir M. Ahmadian (KTH Royal Institute of Technology, Sweden), Matvey Soloviev (KTH Royal Institute of Technology, Sweden), and Musard Balliu (KTH Royal Institute of Technology, Sweden)

Relative Security: Formally Modeling and (Dis)Proving Resilience Against Semantic Optimization Vulnerabilities 403
Brijesh Dongol (University of Surrey, UK), Matt Griffin (University of Surrey, UK), Andrei Popescu (University of Sheffield, UK), and Jamie Wright (University of Sheffield, UK)

Explaining Epsilon in Local Differential Privacy through the Lens of Quantitative Information Flow 419
Natasha Fernandes (Macquarie University, Australia), Annabelle McIver (Macquarie University, Australia), and Parastoo Sadeghi (UNSW Canberra, Australia)

Session 9: Verification 2

Secure Synthesis of Distributed Cryptographic Applications 433
Coşku Acay (Cornell University, USA), Joshua Gancher (Carnegie Mellon University, USA), Rolph Recto (Cornell University, USA), and Andrew Myers (Cornell University, USA)

Synthesizing Tight Privacy and Accuracy Bounds via Weighted Model Counting 449
Lisa Oakley (Northeastern University, USA), Steven Holtzen (Northeastern University, USA), and Alina Oprea (Northeastern University, USA)

Nothing is Out-of-Band: Formal Modeling of Ceremonies 464
Barbara Fila (INSA Rennes, IRISA, France) and Sasa Radomirovic (University of Surrey, United Kingdom)

Session 10: Security Protocols

Software-Based Memory Erasure with relaxed isolation requirements 479
Reynaldo Gil-Pons (University of Luxembourg, Luxembourg), Sergiu Bursuc (University of Luxembourg, Luxembourg), Sjouke Mauw (University of Luxembourg, Luxembourg), and Rolando Trujillo-Rasua (Rovira i Virgili University, Spain)

Dealing with Dynamic Key Compromise in CryptoVerif 495
Bruno Blanchet (Inria, France)

Verification of Correctness and Security Properties for CRYSTALS-KYBER 511
Katharina Kreuzer (Technical University Munich, Germany)

Session 11: Crypto 2

Circuit-Succinct Universally Composable NIZKs with Updatable CRS 527
Behzad Abdolmaleki (University of Sheffield, UK), Noemi Glaeser (University of Maryland, USA & Max Planck Institute for Security and Privacy, Germany), Sebastian Ramacher (AIT Austrian Institute of Technology, Austria), and Daniel Slamanig (Research Institute CODE, Universität der Bundeswehr München, Germany)

Post-quantum Sound CryptoVerif and Verification of Hybrid TLS and SSH Key-Exchanges 543
Bruno Blanchet (Inria) and Charlie Jacomme (Université de Lorraine, CNRS, Inria, LORIA)

Unconditionally Secure MPC for Boolean Circuits with Constant Online Communication 557
Zhenkai Hu (Shanghai Jiao Tong University, China), Kang Yang (State Key Laboratory of Cryptology, China), and Yu Yu (Shanghai Jiao Tong University, China)

UniHand: Privacy-preserving Universal Handover for Small-Cell Networks in 5G-enabled Mobile Communication with KCI Resilience 573
Rabiah Alnashwan (The University of Sheffield, UK - Imam Mohammad Ibn Saud Islamic University, Saudi Arabia), Prosanta Gope (The University of Sheffield, UK), and Benjamin Dowling (The University of Sheffield, UK)

Session 12: Protocols Analysis

Formal Security Analysis of the OpenID FAPI 2.0: Accompanying a Standardization Process 589
Pedram Hosseyni (University of Stuttgart, Germany), Ralf Küsters (University of Stuttgart, Germany), and Tim Würtele (University of Stuttgart, Germany)

Formal Verification of the Sumcheck Protocol 605
Azucena Garvia Bosshard (Independent Researcher), Jonathan Bootle (IBM Research Europe - Zurich), and Christoph Sprenger (ETH Zurich)

Provable Security Analysis of the Secure Remote Password Protocol 620
Dennis Dayanikli (Hasso-Plattner-Institute, University of Potsdam) and Anja Lehmann (Hasso-Plattner-Institute, University of Potsdam)

Solving the Insecurity Problem for Assertions 636
R Ramanujam (Azim Premji University, India), Vaishnavi Sundararajan (IIT Delhi, India), and S P Suresh (Chennai Mathematical Institute, India)

Session 13: Attack Models and Metrics

Urgency in Cybersecurity Risk Management: Toward a Solid Theory 651
Zoltán Ádám Mann (University of Amsterdam)

Attack Tree Metrics are operad Algebras 665
Milan Lopuhaä-Zwakenberg (University of Twente)

Composition in Differential Privacy for General Granularity Notions 680
Patricia Guerra-Balboa (Karlsruhe Institute of Technology, Germany), Àlex Miranda-Pascual (Karlsruhe Institute of Technology, Germany; Universitat Politècnica de Catalunya, Spain), Javier Parra-Arnau (Universitat Politècnica de Catalunya, Spain), and Thorsten Strufe (Karlsruhe Institute of Technology, Germany)

Author Index **697**