

# **2023 IEEE 36th Computer Security Foundations Symposium (CSF 2023)**

**Dubrovnik, Croatia  
9 – 13 July 2023**



**IEEE Catalog Number: CFP23037-POD  
ISBN: 979-8-3503-2193-7**

**Copyright © 2023 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:	CFP23037-POD
ISBN (Print-On-Demand):	979-8-3503-2193-7
ISBN (Online):	979-8-3503-2192-0
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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2023 IEEE 36th Computer Security Foundations Symposium (CSF) **CSF 2023**

## Table of Contents

Preface .....	x
Committees .....	xi

### Cryptography I

Zero-Knowledge in EasyCrypt .....	1
<i>Denis Firsov (Tallinn University of Technology, Estonia / Guardtime, Estonia) and Dominique Unruh (University of Tartu)</i>	
Statement-Oblivious Threshold Witness Encryption .....	17
<i>Sebastian Faust (Technical University of Darmstadt, Germany), Carmit Hazay (Bar-Ilan University, Israel), David Kretzler (Technical University of Darmstadt, Germany), and Benjamin Schlosser (Technical University of Darmstadt, Germany)</i>	
Preimage Awareness in Lincrypt .....	33
<i>Zahra Javar (University of Victoria, Canada) and Bruce Kapron (University of Victoria, Canada)</i>	

### Security Protocols I

Election Verifiability with ProVerif .....	43
<i>Vincent Cheval (Inria Paris, France), Veronique Cortier (Université de Lorraine, Inria, CNRS, France), and Alexandre Debant (Université de Lorraine, Inria, CNRS, France)</i>	
Election Verifiability in Receipt-free Voting Protocols .....	59
<i>Sevdenuur Baloglu (University of Luxembourg, Luxembourg), Sergiu Bursuc (University of Luxembourg, Luxembourg), Sjouke Mauw (University of Luxembourg, Luxembourg), and Jun Pang (University of Luxembourg, Luxembourg)</i>	
Proving Unlinkability using ProVerif through Desynchronised Bi-Processes .....	75
<i>Baelde David (Univ Rennes, CNRS, IRISA, France), Alexandre Debant (Université de Lorraine, CNRS, Inria, Nancy, France), and Stéphanie Delaune (Univ Rennes, CNRS, IRISA, France)</i>	

## Attack Models

Basilic: Resilient-Optimal Consensus Protocols with Benign and Deceitful Faults .....	91
<i>Alejandro Ranchal-Pedrosa (University of Sydney and Protocol Labs) and Vincent Gramoli (University of Sydney and Redbelly Network)</i>	
Towards a Game-Theoretic Security Analysis of Off-Chain Protocols .....	107
<i>Sophie Rain (TU Wien, Austria), Georgia Avarikioti (TU Wien, Austria), Laura Kovács (TU Wien), and Matteo Maffei (Christian Doppler Lab Blockchain Technologies for the Internet of Things, TU Wien, Austria)</i>	
Keep spending: Beyond optimal cyber-security investment .....	123
<i>Yunxiao Zhang (Queen Mary University of London, UK) and Pasquale Malacaria (Queen Mary University of London, UK)</i>	

## Cryptography II

A State-Separating Proof for Yao’s Garbling Scheme .....	137
<i>Chris Brzuska (Aalto University, Finland) and Sabine Oechsner (University of Edinburgh, United Kingdom)</i>	
On the Incoercibility of Digital Signatures .....	153
<i>Ashley Fraser (University of Surrey), Lydia Garms (Keyless Technologies Limited), and Elizabeth A. Quaglia (Royal Holloway, University of London)</i>	
SoK: Delay-based Cryptography .....	169
<i>Liam Medley (Royal Holloway, University of London, United Kingdom), Angelique Faye Loe (Royal Holloway, University of London, United Kingdom), and Elizabeth A. Quaglia (Royal Holloway, University of London, United Kingdom)</i>	

## Security Protocols II

Indistinguishability Beyond Diff-Equivalence in ProVerif .....	184
<i>Vincent Cheval (Inria Paris) and Itsaka Rakotonirina (MPI-SP)</i>	
Subterm-Based Proof Techniques for Improving the Automation and Scope of Security Protocol Analysis .....	200
<i>Cas Cremers (CISPA Helmholtz Center for Information Security, Germany), Charlie Jacomme (CISPA Helmholtz Center for Information Security, Germany), and Philip Lukert (CISPA Helmholtz Center for Information Security, Germany)</i>	
Extending the Authentication Hierarchy with One-Way Agreement .....	214
<i>Johannes Wilson (Sectra Communications, Sweden; Linköping University, Sweden), Mikael Asplund (Linköping University, Sweden), and Niklas Johansson (Sectra Communications, Sweden; Linköping University, Sweden)</i>	

## Blockchain and Smart Contracts

On the (De)centralization of FruitChains .....	229
<i>Aikaterini-Panagiota Stouka (Nethermind, United Kingdom) and Thomas Zacharias (The University of Edinburgh, United Kingdom)</i>	
HoRStify: Sound Security Analysis of Smart Contracts .....	245
<i>Sebastian Holler (Max-Planck-Institute for Security &amp; Privacy; Saarland University), Sebastian Biewer (Saarland University), and Clara Schneidewind (Max-Planck-Institute for Security &amp; Privacy)</i>	
Cross-chain Swaps with Preferences .....	261
<i>Marek Chrobak (University of California at Riverside, United States of America) and Mohsen Lesani (University of California at Riverside, United States of America)</i>	
Smart Contract Synthesis Modulo Hyperproperties .....	276
<i>Norine Coenen (CISPA Helmholtz Center for Information Security, Germany), Bernd Finkbeiner (CISPA Helmholtz Center for Information Security, Germany), Jana Hofmann (CISPA Helmholtz Center for Information Security, Germany), and Julia Tillman (CISPA Helmholtz Center for Information Security, Germany)</i>	

## Language-based Security

OblivIO: Securing reactive programs by oblivious execution with bounded traffic overheads .....	292
<i>Jeppe Fredsgaard Blaabjerg (Aarhus University, Denmark) and Aslan Askarov (Aarhus University, Denmark)</i>	
Robust Safety for Move .....	308
<i>Marco Patrignani (University of Trento) and Sam Blackshear (Mysten Labs)</i>	
Towards End-to-End Verified TEEs via Verified Interface Conformance and Certified Compilers .....	324
<i>Farzaneh Derakhshan (Carnegie Mellon University, USA), Zichao Zhang (Carnegie Mellon University, USA), Amit Vasudevan (Carnegie Mellon University, USA), and Limin Jia (Carnegie Mellon University, USA)</i>	

## Hardware Security

Securing Optimized Code Against Power Side Channels .....	340
<i>Rodothea Myrsini Tsoupidi (Royal Institute of Technology KTH), Roberto Castañeda Lozano (Independent Researcher), Elena Troubitsyna (Royal Institute of Technology KTH), and Panagiotis Papadimitratos (Royal Institute of Technology KTH)</i>	
Formalizing Stack Safety as a Security Property .....	356
<i>Sean Noble Anderson (Portland State University), Roberto Blanco (MPI-SP), Leonidas Lampropoulos (University of Maryland, College Park), Benjamin C. Pierce (University of Pennsylvania), and Andrew Tolmach (Portland State University)</i>	

A Generic Framework to Develop and Verify Security Mechanisms at the Microarchitectural Level: Application to Control-Flow Integrity .....	372
<i>Matthieu Baty (Inria, CNRS, University of Rennes), Pierre Wilke (CentraleSupélec, Inria, CNRS, University of Rennes), Guillaume Hiet (CentraleSupélec, Inria, CNRS, University of Rennes), Arnaud Fontaine (ANSSI, France), and Alix Trieu (ANSSI, France)</i>	

## Quantitative Information Flow (in memory of G. Smith)

Bayes Security: A Not So Average Metric .....	388
<i>Konstantinos Chatzikokolakis (University of Athens), Giovanni Cherubin (Microsoft Research), Catuscia Palamidessi (INRIA, École Polytechnique), and Carmela Troncoso (EPFL)</i>	
Variations and Extensions of Information Leakage Metrics with Applications to Privacy Problems with Imperfect Statistical Information .....	407
<i>Shahnewaz Karim Sakib (Iowa State University, USA), George T Amariuca (Kansas State University, USA), and Yong Guan (Iowa State University, USA)</i>	
Analyzing the Shuffle Model through the Lens of Quantitative Information Flow .....	423
<i>Mireya Jurado (Florida International University, USA), Ramon G. Gonze (Universidade Federal de Minas Gerais, Brazil, and Inria Saclay and École Polytechnique, France), Mário S. Alvim (Universidade Federal de Minas Gerais, Brazil), and Catuscia Palamidessi (Inria Saclay and LIX, École Polytechnique, France)</i>	

## Machine Learning

SoK: Model Inversion Attack Landscape: Taxonomy, Challenges, and Future Roadmap .....	439
<i>Sayanton V. Dibbo (Dartmouth College)</i>	
From Bounded to Unbounded: Privacy Amplification via Shuffling with Dummies .....	457
<i>Shun Takagi (Kyoto University, Japan), Fumiyuki Kato (Kyoto University, Japan), Yang Cao (Hokkaido University, Japan), and Masatoshi Yoshikawa (Osaka Seikei University, Japan)</i>	
Investigating Membership Inference Attacks under Data Dependencies .....	473
<i>Thomas Humphries (University of Waterloo, Canada), Simon Oya (University of Waterloo, Canada), Lindsey Tulloch (University of Waterloo, Canada), Matthew Rafuse (University of Waterloo, Canada), Ian Goldberg (University of Waterloo, Canada), Urs Hengartner (University of Waterloo, Canada), and Florian Kerschbaum (University of Waterloo, Canada)</i>	

## Privacy

Efficient Privacy-Preserving Viral Strain Classification via k-mer Signatures and FHE .....	489
<i>Adi Akavia (University of Haifa, Israel), Ben Galili (Technion, Israel), Hayim Shaul (IBM Research, Israel), Mor Weiss (Bar-Ilan University, Israel), and Zohar Yakhini (Reichman University and Technion, Israel)</i>	

Optimally Hiding Object Sizes with Constrained Padding .....	505
<i>Andrew C. Reed (United States Military Academy, USA) and Michael K. Reiter (Duke University, USA)</i>	

## Language-based Security II

General-Purpose Secure Conflict-free Replicated Data Types .....	521
<i>Bernardo Portela (University of Porto (FCUP) and INESC TEC), Hugo Pacheco (University of Porto (FCUP) and INESC TEC), Pedro Jorge (University of Porto (FCUP)), and Rogério Pontes (INESC TEC)</i>	
pi_RA: A pi-calculus for Verifying Protocols that Use Remote Attestation .....	537
<i>Emiel Lanckriet (KU Leuven, Belgium), Matteo Busi (Ca' Foscari University of Venice, Italy), and Dominique Devriese (KU Leuven)</i>	

## Cryptography III

High-Assurance Field Inversion for Curve-Based Cryptography .....	552
<i>Benjamin Salling Hvass (Aarhus University, Denmark), Diego F. Aranha (Aarhus University, Denmark), and Bas Spitters (Aarhus University, Denmark)</i>	
On Sustainable Ring-based Anonymous Systems .....	568
<i>Sherman S. M. Chow (The Chinese University of Hong Kong, Hong Kong), Christoph Egger (Université Paris Cité, CNRS, IRIF, France), Russell W. F. Lai (Aalto University, Finland), Viktoria Ronge (Friedrich-Alexander University Erlangen-Nuremberg, Germany), and Ivy K. Y. Woo (Aalto University, Finland)</i>	
Collusion-Deterrent Threshold Information Escrow .....	584
<i>Easwar Vivek Mangipudi (Supra Oracles), Donghang Lu (Meta), Alexandros Psomas (Purdue University), and Aniket Kate (Purdue University)</i>	

<b>Author Index</b> .....	<b>601</b>
---------------------------	------------