

# **2021 IEEE 34th Computer Security Foundations Symposium (CSF 2021)**

**Dubrovnik, Croatia  
21 – 25 June 2021**



**IEEE Catalog Number: CFP21037-POD  
ISBN: 978-1-7281-7608-6**

**Copyright © 2021 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:	CFP21037-POD
ISBN (Print-On-Demand):	978-1-7281-7608-6
ISBN (Online):	978-1-7281-7607-9
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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# TABLE OF CONTENTS

DYNAMIC IFC THEOREMS FOR FREE!.....	1
<i>Maximilian Alghed, Jean-Philippe Bernardy, Catalin Hritcu</i>	
AUTOMATING AUDIT WITH POLICY INFERENCE .....	15
<i>Abhishek Bichhawat, Matt Fredrikson, Jean Yang</i>	
STATISTICAL MODEL CHECKING FOR HYPERPROPERTIES .....	31
<i>Yu Wang, Siddhartha Nalluri, Borzoo Bonakdarpour, Miroslav Pajic</i>	
KACHINA – FOUNDATIONS OF PRIVATE SMART CONTRACTS .....	47
<i>Thomas Kerber, Aggelos Kiayias, Markulf Kohlweiss</i>	
HEURISTIC APPROACH FOR COUNTERMEASURE SELECTION USING ATTACK GRAPHS .....	63
<i>Orly Stan, Ron Bitton, Michal Ezrets, Moran Dadon, Masaki Inokuchi, Yoshinobu Ohta, Tomohiko Yagyu, Yuval Elovici, Asaf Shabtai</i>	
ON COMPOSITIONAL INFORMATION FLOW AWARE REFINEMENT .....	79
<i>Christoph Baumann, Mads Dam, Roberto Guanciale, Hamed Nemati</i>	
ACCOUNTABILITY IN THE DECENTRALISED-ADVERSARY SETTING .....	95
<i>Robert Künnemann, Deepak Garg, Michael Backes</i>	
RESOURCE-AWARE SESSION TYPES FOR DIGITAL CONTRACTS.....	111
<i>Ankush Das, Stephanie Balzer, Jan Hoffmann, Frank Pfening, Ishani Santurkar</i>	
CONCISE UC ZERO-KNOWLEDGE PROOFS FOR OBLIVIOUS UPDATABLE DATABASES .....	127
<i>Jan Camenisch, Maria Dubovitskaya, Alfredo Rial</i>	
PERFORMING SECURITY PROOFS OF STATEFUL PROTOCOLS .....	143
<i>Andreas V. Hess, Sebastian Mödersheim, Achim D. Brucker, Anders Schlichtkrull</i>	
FORMAL VERIFICATION OF SECURE FORWARDING PROTOCOLS .....	159
<i>Tobias Klenze, Christoph Sprenger, David Basin</i>	
FIXING THE ACHILLES HEEL OF E-VOTING: THE BULLETIN BOARD .....	175
<i>Lucca Hirschi, Lara Schmid, David Basin</i>	
COMPUTATIONALLY SOUND BITCOIN TOKENS .....	192
<i>Massimo Bartoletti, Stefano Lande, Roberto Zunino</i>	
SECURE COMPILATION OF CONSTANT-RESOURCE PROGRAMS .....	207
<i>Gilles Barthe, Sandrine Blazy, Rémi Hutin, David Pichardie</i>	
CONCAVITY, CORE-CONCAVITY, QUASICONCAVITY: A GENERALIZING FRAMEWORK FOR ENTROPY MEASURES .....	219
<i>Arthur Américo, Pasquale Malacaria</i>	
VERIFYING HYPERPROPERTIES WITH TLA .....	233
<i>Leslie Lamport, Fred B. Schneider</i>	
GRADUAL SECURITY TYPES AND GRADUAL GUARANTEES .....	249
<i>Abhishek Bichhawat, McKenna McCall, Limin Jia</i>	

A COQ PROOF OF THE CORRECTNESS OF X25519 IN TWEETNACL.....	265
<i>Peter Schwabe, Benoît Viguier, Timmy Weerwag, Freek Wiedijk</i>	
ELECTION VERIFIABILITY REVISITED: AUTOMATED SECURITY PROOFS AND ATTACKS ON HELIOS AND BELENIOS .....	281
<i>Sevdenuur Baloglu, Sergiu Bursuc, Sjouke Mauw, Jun Pang</i>	
BACKWARDS-DIRECTED INFORMATION FLOW ANALYSIS FOR CONCURRENT PROGRAMS .....	296
<i>Kirsten Winter, Nicholas Coughlin, Graeme Smith</i>	
MACHINE-CHECKING UNFORGEABILITY PROOFS FOR SIGNATURE SCHEMES WITH TIGHT REDUCTIONS TO THE COMPUTATIONAL DIFFIE-HELLMAN PROBLEM.....	312
<i>François Dupressoir, Sara Zain</i>	
VERIFYING ACCOUNTABILITY FOR UNBOUNDED SETS OF PARTICIPANTS .....	327
<i>Kevin Morio, Robert Künnemann</i>	
TOWARDS LANGUAGE-BASED MITIGATION OF TRAFFIC ANALYSIS ATTACKS.....	343
<i>Jeppé Fredsgaard Blaabjerg, Aslan Askarov</i>	
A QUANTALE OF INFORMATION.....	358
<i>Sebastian Hunt, David Sands</i>	
EFFICIENT CONSTRUCTIONS OF PAIRING BASED ACCUMULATORS .....	373
<i>Ioanna Karantaidou, Foteini Baldimtsi</i>	
COOKING CRYPTOGRAPHERS: SECURE MULTIPARTY COMPUTATION BASED ON BALLS AND BAGS .....	389
<i>Daiki Miyahara, Yuichi Komano, Takaaki Mizuki, Hideaki Sone</i>	
RELATIONAL ANALYSIS OF SENSOR ATTACKS ON CYBER-PHYSICAL SYSTEMS .....	405
<i>Jian Xiang, Nathan Fulton, Stephen Chong</i>	
CAPABLEPTRS: SECURELY COMPILING PARTIAL PROGRAMS USING THE POINTERS- AS-CAPABILITIES PRINCIPLE.....	421
<i>Akram El-Korashy, Stelios Tsampas, Marco Patrignani, Dominique Devriese, Deepak Garg, Frank Piessens</i>	
LANGUAGE SUPPORT FOR SECURE SOFTWARE DEVELOPMENT WITH ENCLAVES.....	437
<i>Aditya Oak, Amir M. Ahmadian, Musard Balliu, Guido Salvaneschi</i>	
VERTICAL COMPOSITION AND SOUND PAYLOAD ABSTRACTION FOR STATEFUL PROTOCOLS.....	453
<i>Sébastien Gondron, Sebastian Mödersheim</i>	
ON THE SOUNDNESS OF INFRASTRUCTURE ADVERSARIES.....	469
<i>Alexander Dax, Robert Künnemann</i>	
FORMAL IMPACT METRICS FOR CYBER-PHYSICAL ATTACKS .....	485
<i>Ruggero Lanotte, Massimo Merro, Andrei Munteanu, Simone Tini</i>	
EFFICIENT ALGORITHMS FOR QUANTITATIVE ATTACK TREE ANALYSIS .....	501
<i>Carlos E. Budde, Mariëlle Stoelinga</i>	
FORMALIZING NAKAMOTO-STYLE PROOF OF STAKE.....	516
<i>Søren Eller Thomsen, Bas Spitters</i>	

DDUO: GENERAL-PURPOSE DYNAMIC ANALYSIS FOR DIFFERENTIAL PRIVACY .....	531
<i>Chike Abuah, Alex Silence, David Darais, Joseph P. Near</i>	
YES WE CAN: WATERMARKING MACHINE LEARNING MODELS BEYOND CLASSIFICATION.....	546
<i>Sofiane Lounici, Mohamed Njeh, Orhan Ermis, Melek Önen, Slim Trabelsi</i>	
CONSISTENCY FOR FUNCTIONAL ENCRYPTION .....	560
<i>Christian Badertscher, Aggelos Kiayias, Markulf Kohlweiss, Hendrik Waldner</i>	
A FORMAL INFORMATION-THEORETIC LEAKAGE ANALYSIS OF ORDER-REVEALING ENCRYPTION.....	576
<i>Mireya Jurado, Catuscia Palamidessi, Geoffrey Smith</i>	
ABSTRACT MODELING OF SYSTEM COMMUNICATION IN CONSTRUCTIVE CRYPTOGRAPHY USING CRYPTHOL.....	592
<i>David Basin, Andreas Lochbihler, Ueli Maurer, S. Reza Sefidgar</i>	
SSPROVE: A FOUNDATIONAL FRAMEWORK FOR MODULAR CRYPTOGRAPHIC PROOFS IN COQ .....	608
<i>Carmine Abate, Philipp G. Haselwarter, Exequiel Rivas, Antoine Van Muylder, Théo Winterhalter, Catalin Hritcu, Kenji Maillard, Bas Spitters</i>	
MECHANISED MODELS AND PROOFS FOR DISTANCE-BOUNDING .....	623
<i>Ioana Boureanu, Constantin Catalin Dragan, François Dupressoir, David Gérard, Pascal Lafourcade</i>	
FORMAL SECURITY ANALYSIS OF MPC-IN-THE-HEAD ZERO-KNOWLEDGE PROTOCOLS.....	639
<i>Nikolaj Sidorenko, Sabine Oechsner, Bas Spitters</i>	
VERIFIED MULTIPLE-TIME SIGNATURE SCHEME FROM ONE-TIME SIGNATURES AND TIMESTAMPING.....	653
<i>Denis Firsov, Henri Lakk, Ahto Truu</i>	

**Author Index**