

Lecture Notes in Computer Science

13950

Founding Editors


Gerhard Goos

Juris Hartmanis

Editorial Board Members

Elisa Bertino, *Purdue University, West Lafayette, IN, USA*

Wen Gao, *Peking University, Beijing, China*

Bernhard Steffen , *TU Dortmund University, Dortmund, Germany*

Moti Yung , *Columbia University, New York, NY, USA*

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.


LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.


Foteini Baldimtsi · Christian Cachin
Editors

Financial Cryptography and Data Security

27th International Conference, FC 2023
Bol, Brač, Croatia, May 1–5, 2023
Revised Selected Papers, Part I

Editors

Foteini Baldimtsi 
George Mason University
Fairfax, VA, USA

Christian Cachin 
University of Bern
Bern, Switzerland

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-47753-9

ISBN 978-3-031-47754-6 (eBook)

<https://doi.org/10.1007/978-3-031-47754-6>

© International Financial Cryptography Association 2024

Chapter “Optimally-Fair Exchange of Secrets via Delay Encryption and Commutative Blinding” is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapter.

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Preface

The 27th International Conference on Financial Cryptography and Data Security, FC 2023, was held from May 1 to May 5, 2023, at the Bluesun Hotel Elaphusa in Bol, on the island of Brač, Croatia. The conference is organized annually by the International Financial Cryptography Association (IFCA).

We received 182 papers (165 regular ones and 17 short papers) by the submission deadline for the conference, which was October 19th, 2022. Of these, 41 were accepted (39 regular papers and two short papers), resulting in an acceptance rate of 22.5%. The present proceedings volume contains revised versions of all the papers presented at the conference.

The review process lasted approximately two months and was double-blind. Each paper received a minimum of three reviews. The Program Committee used the HotCRP system to organize the reviewing process. The merits of each paper were discussed thoroughly and intensely on the online platform as we converged to the final decisions. In the end, a number of worthy papers still had to be rejected owing to the limited number of slots in the conference program.

The Program Committee (PC) consisted of 64 members with expertise in various aspects of financial cryptography, including representatives from both industry and academia. The PC additionally solicited reviews from 58 external reviewers. We are deeply grateful to all the members of the PC and the external reviewers for their dedication and thorough work. Their valuable insights and constructive feedback considerably strengthened the overall quality of the final program.

The main conference program lasted for four days. A half-day tutorial on the topic of “Constant Function Market Makers” took place a day before the main conference and a series of one-day workshops were held the day after the main conference. The main conference started with an invited keynote talk by George Danezis, University College London and Mysten Labs, titled “Combining broadcast and consensus in a production blockchain system.” The accepted papers were presented in 10 sessions and there was also a Rump Session and a General Meeting. Finally, two posters were presented during the poster session.

We are grateful to the general chairs, Ray Hirschfeld and Carla Mascia, for an excellent organization. Additionally, we appreciate the dedication of the IFCA directors and Steering Committee for their service. We would also like to express our thankfulness to the conference sponsors whose generous support made this event possible. Our Platinum Sponsors: a16z Crypto Research, Casper Association, Chainlink Labs and Mysten Labs. Our Silver Sponsors: Evertas and Zcash Foundation. Finally, we would like to thank our sponsors in kind: the Croatian National Tourist Board, the Split-Dalmatia Tourist Board, the Bol Tourist Board, and Worldpay.

Lastly, our sincere gratitude goes to all the authors who submitted their papers to this conference, as well as to all the attendees who contributed to making this event a truly

intellectually stimulating experience through their active participation. Their support is the most important factor for the success of the conference.

August 2023

Foteini Baldimtsi
Christian Cachin

Organization

General Chairs

Rafael Hirschfeld
Carla Mascia

Unipay Technologies, The Netherlands
University of Trento, Italy

Steering Committee

Joseph Bonneau

New York University and a16z Crypto Research,
USA

Sven Dietrich

City University of New York, USA

Rafael Hirschfeld

Unipay Technologies, The Netherlands

Andrew Miller

University of Illinois at Urbana-Champaign, USA

Monica Quaintance

Zenia Systems, USA

Burton Rosenberg

University of Miami, USA

Kazue Sako

Waseda University, Japan

Program Committee Chairs

Foteini Baldimtsi
Christian Cachin

George Mason University, USA
University of Bern, Switzerland

Program Committee

Ghada Almashaqbeh

University of Connecticut, USA

Zeta Avarikioti

Technical University of Vienna, Austria

Christian Badertscher

Input Output, Switzerland

Massimo Bartoletti

University of Cagliari, Italy

Rainer Böhme

University of Innsbruck, Austria

Joseph Bonneau

New York University and a16z Crypto Research,
USA

Benedikt Bünz

Stanford University and Espresso Systems, USA

L. Jean Camp

Indiana University, USA

Srdjan Čapkun

ETH Zurich, Switzerland

Kostas Chalkias

Mysten Labs, USA

T.-H. Hubert Chan

University of Hong Kong, China

Panagiotis Chatzigiannis

Visa Research, USA

Jeremy Clark	Concordia University, Canada
Vanesa Daza	Universitat Pompeu Fabra, Spain
Rafael Dowsley	Monash University, Australia
Stefan Dziembowski	University of Warsaw, Poland
Karim Eldefrawy	SRI International, USA
Kaoutar Elkhayaoui	IBM Research, Switzerland
Zeki Erkin	TU Delft, The Netherlands
Chaya Ganesh	Indian Institute of Science, Bangalore, India
Christina Garman	Purdue University, USA
Peter Gaži	Input Output, Slovakia
Rosario Gennaro	Protocol Labs, USA
Arthur Gervais	University College London, UK
Ethan Heilman	BastionZero, USA
Ari Juels	Cornell Tech, USA
Aniket Kate	Purdue University and Supra Research, USA
Lefteris Kokoris-Kogias	IST Austria, Austria
Evgenios M. Kornaropoulos	George Mason University, USA
Duc V. Le	University of Bern, Switzerland
Andrew Lewis-Pye	London School of Economics, UK
Ben Livshits	Imperial College and Brave Software, UK
Giorgia Azzurra Marson	NEC Labs Europe, Germany
Shin'ichiro Matsuo	Georgetown University, USA
Patrick McCorry	Infura, UK
Ian Miers	University of Maryland, USA
Andrew Miller	University of Illinois at Urbana-Champaign, USA
Pedro Moreno-Sanchez	IMDEA Software Institute, Spain
Kartik Nayak	Duke University, USA
Valeria Nikolaenko	a16z Crypto Research, USA
Anca Nitulescu	Protocol Labs, France
Giorgos Panagiotakos	Input Output, UK
Dimitris Papadopoulos	Hong Kong University of Science and Technology, China
Charalampos Papamanthou	Yale University, USA
Alexandros Psomas	Purdue University, USA
Elizabeth A. Quaglia	Royal Holloway, University of London, UK
Ling Ren	University of Illinois at Urbana-Champaign, USA
Ori Rottenstreich	Technion, Israel
Abhi Shelat	Northeastern University, USA
Alberto Sonnino	Mysten Labs, UK
Alessandro Sorniotti	IBM Research, Switzerland
Alexander Spiegelman	Aptos Labs, USA
Chrysoula Stathakopoulou	Chainlink Labs, Switzerland

Vanessa Teague	Thinking Cybersecurity and Australian National University, Australia
Marie Vasek	University College London, UK
Roger Wattenhofer	ETH Zurich, Switzerland
Edgar Weippl	University of Vienna and SBA Research, Austria
Fan Zhang	Yale University, USA
Haibin Zhang	Beijing Institute of Technology, China
Ren Zhang	Cryptape Co. Ltd. and Nervos, China
Yupeng Zhang	Texas A&M University, USA
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Dionysis Zindros	Stanford University, USA
Aviv Zohar	Hebrew University, Israel

Additional Reviewers

Hamza Abusalah	Joël Mathys
Amit Agarwal	Subhra Mazumdar
Jannik Albrecht	Liam Medley
Balaji Arun	Jovana Micic
Judith Beestermöller	Atsuki Momose
Adithya Bhat	Muhammad Haris Mudgees
Matteo Campanelli	Kamilla Nazirkhanova
Kevin Choi	Ben Riva
Sandro Coretti-Drayton	Schwinn Saereesitthipitak
Xiaohai Dai	Philipp Schindler
Sourav Das	Peiyao Sheng
Yepeng Michael Ding	Srivatsan Sridhar
Fatima Elsheimy	Shravan Srinivasan
Zhiyong Fang	Christo Stefo
Rati Gelashvili	Nicholas Stifter
Tiantian Gong	Ertem Nusret Tas
Florian Grötschla	Benjamin Turner
Lioba Heimbach	Athina Terzoglou
Javier Herranz	Phuc Thai
Yanxue Jia	Giorgos Tsimos
Aljosha Judmayer	Sarisht Wadhwa
Dimitris Karakostas	Chenghong Wang
David Lehnher	Weijie Wang
Rujia Li	Zhuolun Xiang
Yunqi Li	Yuting Xiao
Yujie Lu	Tom Yurek
Zhichun Lu	Yuncong Zhang
Nikos Makriyannis	Ren Zhijie
Easwar Vivek Mangipudi	Zhelei Zhou
Deepak Maram	

Contents – Part I

Consensus

Executing and Proving Over Dirty Ledgers	3
<i>Christos Stefo, Zhuolun Xiang, and Lefteris Kokoris-Kogias</i>	
Byzantine Generals in the Permissionless Setting	21
<i>Andrew Lewis-Pye and Tim Roughgarden</i>	
The Unique Chain Rule and Its Applications	38
<i>Adithya Bhat, Akhil Bandarupalli, Saurabh Bagchi, Aniket Kate, and Michael K. Reiter</i>	
Player-Replaceability and Forensic Support Are Two Sides of the Same (Crypto) Coin	56
<i>Peiyao Sheng, Gerui Wang, Kartik Nayak, Sreeram Kannan, and Pramod Viswanath</i>	

Cryptographic Protocols

Synchronous Perfectly Secure Message Transmission with Optimal Asynchronous Fallback Guarantees	77
<i>Giovanni Deligios and Chen-Da Liu-Zhang</i>	
Optimally-Fair Exchange of Secrets via Delay Encryption and Commutative Blinding	94
<i>Ivo Maffei and Andrew W. Roscoe</i>	
Witness-Authenticated Key Exchange, Revisited: Extensions to Groups, Improved Models, Simpler Constructions	112
<i>Matteo Campanelli, Rosario Gennaro, Kelsey Melissaris, and Luca Nizzardo</i>	
On the Correlation Complexity of MPC with Cheater Identification	129
<i>Nicholas Brandt, Sven Maier, Tobias Müller, and Jörn Müller-Quade</i>	
TALUS: Reinforcing TEE Confidentiality with Cryptographic Coprocessors	147
<i>Dhiman Chakraborty, Michael Schwarz, and Sven Bugiel</i>	

Practical Construction for Secure Trick-Taking Games Even with Cards Set Aside	166
<i>Rohann Bella, Xavier Bultel, Céline Chevalier, Pascal Lafourcade, and Charles Olivier-Anclin</i>	
Signature for Objects: Formalizing How to Authenticate Physical Data and More	182
<i>Ryuya Hayashi, Taiki Asano, Junichiro Hayata, Takahiro Matsuda, Shota Yamada, Shuichi Katsumata, Yusuke Sakai, Tadanori Teruya, Jacob C. N. Schuldt, Nuttapong Attrapadung, Goichiro Hanaoka, Kanta Matsuura, and Tsutomu Matsumoto</i>	
The Superlinearity Problem in Post-quantum Blockchains	200
<i>Sunoo Park and Nicholas Spooner</i>	
Fair Delivery of Decentralised Randomness Beacon	218
<i>Runchao Han and Jiangshan Yu</i>	
Bicorn: An Optimistically Efficient Distributed Randomness Beacon	235
<i>Kevin Choi, Arasu Arun, Nirvan Tyagi, and Joseph Bonneau</i>	
McFly: Verifiable Encryption to the Future Made Practical	252
<i>Nico Döttling, Lucjan Hanzlik, Bernardo Magri, and Stella Wahnig</i>	
Eagle: Efficient Privacy Preserving Smart Contracts	270
<i>Carsten Baum, James Hsin-yu Chiang, Bernardo David, and Tore Kasper Frederiksen</i>	
Provably Avoiding Geographic Regions for Tor’s Onion Services	289
<i>Arushi Arora, Raj Karra, Dave Levin, and Christina Garman</i>	
Decentralized Finance	
R2: Boosting Liquidity in Payment Channel Networks with Online Admission Control	309
<i>Mahsa Bastankhah, Krishnendu Chatterjee, Mohammad Ali Maddah-Ali, Stefan Schmid, Jakub Svoboda, and Michelle Yeo</i>	
Complexity-Approximation Trade-Offs in Exchange Mechanisms: AMMs vs. LOBs	326
<i>Jason Milonidis, Ciamac C. Moallemi, and Tim Roughgarden</i>	

Mitigating Decentralized Finance Liquidations with Reversible Call Options	344
<i>Kaihua Qin, Jens Ernstberger, Liyi Zhou, Philipp Jovanovic, and Arthur Gervais</i>	
Short Paper: DeFi Deception—Uncovering the Prevalence of Rugpulls in Cryptocurrency Projects	363
<i>Sharad Agarwal, Gilberto Atondo-Siu, Marilyne Ordekian, Alice Hutchings, Enrico Mariconti, and Marie Vasek</i>	
Author Index	373

Contents – Part II

Proof of X

SNACKs for Proof-of-Space Blockchains	3
<i>Hamza Abusalah</i>	
Proof of Necessary Work: Succinct State Verification with Fairness Guarantees	18
<i>Assimakis Kattis and Joseph Bonneau</i>	
Proof of Availability and Retrieval in a Modular Blockchain Architecture	36
<i>Shir Cohen, Guy Goren, Lefteris Kokoris-Kogias, Alberto Sonnino, and Alexander Spiegelman</i>	
Limits on Revocable Proof Systems, With Implications for Stateless Blockchains	54
<i>Miranda Christ and Joseph Bonneau</i>	

Layer 2

State Machines Across Isomorphic Layer 2 Ledgers	75
<i>Maxim Jourenko and Mario Larangeira</i>	
Get Me Out of This Payment! Bailout: An HTLC Re-routing Protocol	92
<i>Oğuzhan Ersoy, Pedro Moreno-Sanchez, and Stefanie Roos</i>	
Extras and Premiums: Local PCN Routing with Redundancy and Fees	110
<i>Yu Shen, Oğuzhan Ersoy, and Stefanie Roos</i>	
An Efficient Algorithm for Optimal Routing Through Constant Function Market Makers	128
<i>Theo Diamandis, Max Resnick, Tarun Chitra, and Guillermo Angeris</i>	

Attack Techniques, Defenses, and Attack Case Studies

Leveraging the Verifier’s Dilemma to Double Spend in Bitcoin	149
<i>Tong Cao, Jérémie Decouchant, and Jiangshan Yu</i>	
On the Sustainability of Bitcoin Partitioning Attacks	166
<i>Jaehyun Ha, Seungjin Baek, Muoi Tran, and Min Suk Kang</i>	

Demystifying Web3 Centralization: The Case of Off-Chain NFT Hijacking	182
<i>Felix Stöger, Anxin Zhou, Huayi Duan, and Adrian Perrig</i>	
Defending Against Free-Riders Attacks in Distributed Generative Adversarial Networks	200
<i>Zilong Zhao, Jiyue Huang, Lydia Y. Chen, and Stefanie Roos</i>	
Empirical Studies and more Decentralized Finance	
Dissecting Bitcoin and Ethereum Transactions: On the Lack of Transaction Contention and Prioritization Transparency in Blockchains	221
<i>Johnnatan Messias, Vabuk Pahari, Balakrishnan Chandrasekaran, Krishna P. Gummadi, and Patrick Loiseau</i>	
Forstage: Anatomy of a Smart-Contract Pyramid Scheme	241
<i>Tyler Kell, Haaron Yousaf, Sarah Allen, Sarah Meiklejohn, and Ari Juels</i>	
Understanding Polkadot Through Graph Analysis: Transaction Model, Network Properties, and Insights	259
<i>Hanaa Abbas, Maurantonio Caprolu, and Roberto Di Pietro</i>	
Short Paper: Estimating Patch Propagation Times Across Blockchain Forks	276
<i>Sébastien Andreina, Lorenzo Alluminio, Giorgia Azzurra Marson, and Ghassan Karame</i>	
Game Theory and Protocols	
DeFi and NFTs Hinder Blockchain Scalability	291
<i>Lioba Heimbach, Quentin Kniep, Yann Vonlanthen, and Roger Wattenhofer</i>	
Cryptoeconomic Security for Data Availability Committees	310
<i>Ertem Nusret Tas and Dan Boneh</i>	
Kadabra: Adapting Kademlia for the Decentralized Web	327
<i>Yunqi Zhang and Shaileshh Bojja Venkatakrishnan</i>	
Optimality Despite Chaos in Fee Markets	346
<i>Stefanos Leonardos, Daniël Reijsbergen, Barnabé Monnot, and Georgios Piliouras</i>	
Author Index	363