

Ittay Eyal
Juan Garay (Eds.)

LNCS 13411

Financial Cryptography and Data Security

26th International Conference, FC 2022
Grenada, May 2–6, 2022
Revised Selected Papers



 **Springer**

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

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

More information about this series at <https://link.springer.com/bookseries/558>

Ittay Eyal · Juan Garay (Eds.)

Financial Cryptography and Data Security

26th International Conference, FC 2022

Grenada, May 2–6, 2022

Revised Selected Papers

Editors

Ittay Eyal 
Technion - Israel Institute of Technology
Haifa, Israel

Juan Garay 
Texas A&M University
College Station, TX, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-18282-2 ISBN 978-3-031-18283-9 (eBook)
<https://doi.org/10.1007/978-3-031-18283-9>

© International Financial Cryptography Association 2022

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

Preface

The 26th International Conference on Financial Cryptography and Data Security (FC 2022) was held on the beautiful island of Grenada from May 2 to May 6, 2022. The conference is organized annually by the International Financial Cryptography Association (IFCA) and is a major international forum for research, advanced development, education, exploration, and debate regarding information assurance, with a specific focus on financial and commercial contexts. The conference aims to attract works focusing on both fundamental and real-world deployments on all aspects surrounding commerce security.

The conference was supposed to take place earlier, from February 14 to February 18, 2022, but due to uncertainties related to COVID-19, the conference’s Steering Committee decided to postpone it. This turned out to be a prophetic decision as by the beginning of May many travel restrictions had been lifted, resulting in a lively and well-attended conference, a much-needed experience after the long COVID-19 hiatus.

These proceedings include the 36 papers that were selected by the Program Committee (PC), out of a total of 159 received submissions. Submissions were assigned to at least three reviewers, while submissions by PC members were assigned at least four reviews. The double blind review process and ensuing discussion among PC members were lively and engaging, to the extent that 15 of the accepted papers were conditionally accepted and shepherded by selected PC members. Five of the accepted manuscripts are short papers and one is a Systematization of Knowledge (SoK) contribution. In addition, we received four poster submissions, out of which three were accepted, but, due to travel impediments, only one was displayed during the Welcome Reception and Poster Session on Monday evening.

This year the Program Committee consisted of 64 members, and we made every attempt for its composition to reflect our proficiency, diversity, and inclusion goals. We are deeply grateful to the members of the PC for their dedication and thorough work, as well as to the many external reviewers who joined the review process in their areas of expertise.

FC 2022 celebrated 25 years of the FC conference program (postponed from last year’s 25th FC that was online only due to COVID-19). The program was enriched by a special anniversary program and included a “Looking back at 25 years of FC history” presentation assembled by Kazue Sako and delivered by Sven Dietrich; a “Perspectives from FC since 2015” anniversary talk by Patrick McCorry; FC 25th anniversary vignettes collected by the anniversary coordinators; and a FC 25th anniversary retrospective panel—past impact and going forward, with panelists Don Beaver, Andrew Miller, and Hinde ten Berge, moderated by Sven Dietrich.

The main conference program, which lasted four days, was followed by a series of one-day workshops and a tutorial on more specialized topics: AMHIS 2022 (1st Workshop on Approaches to Modelling Heterogeneous Interacting Systems), CoDecFin 2022 (3rd Workshop on Coordination of Decentralized Finance), DeFi 2022 (2nd Workshop on Decentralized Finance), Voting 2022 (7th Workshop on Advances in

Secure Electronic Voting), WTSC 2022 (6th Workshop on Trusted Smart Contracts), and the “Quantum Computing Essentials for Financial Cryptographers” tutorial given by Or Sattath.

We are grateful to General Chairs Sergi Delgado Segura and Rafael (Ray) Hirschfeld for their predisposition, availability and efforts. In fact, it is hard to think of an aspect of the event’s organization—from managing the conference’s website, and collecting and uploading the talks’ videos to YouTube, to coordinating all the fluctuating dates, updates, and related logistics with the Radisson Grenada Beach Resort hotel where the conference took place—which Ray wasn’t on top of, and which resulted in such a well-planned and enjoyable event—thanks, Ray!

We are also grateful to the conference Platinum sponsors (Casper, CipherTrace, Harmony, Novi, and Ripple); to the Gold Sponsors (Chainalysis, IBM Research, Interlay, and Zilliqa); to the Silver Sponsors (IOHK, Manta Ray Labs, NTT Research, Protocol Labs, Smart Contract Research Forum, and the Zcash Foundation); and to the Sponsors in Kind (Grenada Tourism Authority and Worldpay), as well as the Uniswap Grant Program.

Finally, we thank all the authors who submitted papers to this conference, and all the conference attendees who made this event a truly intellectually stimulating one through their active participation.

August 2022

Ittay Eyal
Juan Garay

Organization

General Chairs

Sergi Delgado Segura
Rafael Hirschfeld

Talaia Labs, UK
Unipay Technologies, The Netherlands

Program Committee Chairs

Ittay Eyal
Juan Garay

Technion, Israel
Texas A&M University, USA

Steering Committee

Joseph Bonneau
Rafael Hirschfeld
Andrew Miller
Monica Quaintance
Burton Rosenberg

New York University, USA
Unipay Technologies, The Netherlands
University of Illinois at Urbana-Champaign, USA
Zenia Systems, USA
University of Miami, USA

Program Committee

Ittai Abraham
Christian Badertscher
Foteini Baldimtsi
Jeremiah Blocki
Rainer Böhme
Joseph Bonneau
Christian Cachin
L. Jean Camp
Srdjan Capkun
Hubert Chan
Jing Chen
Michele Ciampi
Jeremy Clark
Vanesa Daza
Stefan Dziembowski
Karim Eldefrawy
Matthias Fitzi

VMware Research, Israel
IOHK, Switzerland
George Mason University, USA
Purdue University, USA
University of Innsbruck, Austria
New York University, USA
University of Bern, Switzerland
Indiana University, USA
ETH Zurich, Switzerland
University of Hong Kong, China
Stony Brook University, USA
University of Edinburgh, UK
Concordia University, Canada
Pompeu Fabra University, Spain
University of Warsaw, Poland
SRI International, USA
IOHK, Switzerland

Chaya Ganesh	Indian Institute of Science, Bangalore, India
Christina Garman	Purdue University, USA
Arthur Gervais	Imperial College London, UK
Stephanie Hurder	Prysm Group, USA
Ari Juels	Cornell Tech, USA
Aniket Kate	Purdue University, USA
Eleftherios Kokoris Kogias	IST Austria and Novi Research, Austria
Nikos Leonardos	National and Kapodistrian University of Athens, Greece
Ben Livshits	Imperial College London and Brave Software, UK
Daniel Masny	Visa Research, USA
Shin'ichiro Matsuo	Georgetown University and NTT Research, USA
Patrick McCorry	Infura, UK
Shagufta Mehnaz	Dartmouth College, USA
Ian Miers	University of Maryland, USA
Andrew Miller	University of Illinois at Urbana-Champaign, USA
Tal Moran	IDC, Israel
Pedro Moreno-Sanchez	IMDEA Software Institute, Spain
Pratyay Mukherjee	Visa Research, USA
Kartik Nayak	Duke University, USA
Georgios Panagiotakos	IOHK, Greece
Benny Pinkas	Bar-Ilan University, Israel
Alex Psomas	Purdue University, USA
Elizabeth Quaglia	Royal Holloway, University of London, UK
Ling Ren	University of Illinois at Urbana-Champaign, USA
Ori Rottenstreich	Technion, Israel
Mahmood Sharif	Tel Aviv University, Israel
Abhi Shelat	Northeastern University, USA
Mark Simkin	Aarhus University, Denmark
Alessandro Sorniotti	IBM Research – Zurich, Switzerland
Alexander Spiegelman	Novi Research, Israel
Ewa Syta	Trinity College, USA
Qiang Tang	University of Sydney, Australia
Vanessa Teague	Thinking Cybersecurity and the Australian National University, Australia
Daniel Tschudi	Concordium, Switzerland
David Tse	Stanford University, USA
Marko Vukolic	Protocol Labs, Switzerland
Riad Wahby	Stanford University and Algorand, USA
Roger Wattenhofer	ETH Zurich, Switzerland
Edgar Weippl	University of Vienna and SBA Research, Austria
Fan Zhang	Duke University, USA

Ren Zhang
Yupeng Zhang
Hong-Sheng Zhou
Vassilis Zikas
Aviv Zohar

Nervos, USA
Texas A&M University, USA
Virginia Commonwealth University, USA
Purdue University, USA
The Hebrew University, Israel

Contents

Tokenomics

- Maximizing Extractable Value from Automated Market Makers 3
Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente
- Kicking-the-Bucket: Fast Privacy-Preserving Trading Using Buckets 20
Mariana Botelho da Gama, John Carlidge, Antigoni Polychroniadou, Nigel P. Smart, and Younes Talibi Alaoui
- Speculative Multipliers on DeFi: Quantifying On-Chain Leverage Risks 38
Zhipeng Wang, Kaihua Qin, Duc Vu Minh, and Arthur Gervais

MPC (Mostly)

- Explainable Arguments 59
Lucjan Hanzlik and Kamil Kluczniak
- MPCCache: Privacy-Preserving Multi-Party Cooperative Cache Sharing at the Edge 80
Duong Tung Nguyen and Ni Trieu
- Multi-party Updatable Delegated Private Set Intersection 100
Aydin Abadi, Changyu Dong, Steven J. Murdoch, and Sotirios Terzis

Privacy

- The Effect of False Positives: Why Fuzzy Message Detection Leads to Fuzzy Privacy Guarantees? 123
István András Seres, Balázs Pejő, and Péter Burcsi
- Differential Privacy in Constant Function Market Makers 149
Tarun Chitra, Guillermo Angeris, and Alex Evans
- Anonymous Tokens with Public Metadata and Applications to Private Contact Tracing 179
Tjerand Silde and Martin Strand

ZKP

SnarkPack: Practical SNARK Aggregation 203
Nicolas Gailly, Mary Maller, and Anca Nitulescu

On Interactive Oracle Proofs for Boolean R1CS Statements 230
Ignacio Cascudo and Emanuele Giunta

Zero Knowledge Proofs Towards Verifiable Decentralized AI Pipelines 248
Nitin Singh, Pankaj Dayama, and Vinayaka Pandit

Old-School Consensus

Be Aware of Your Leaders 279
Shir Cohen, Rati Gelashvili, Lefteris Kokoris Kogias, Zekun Li, Dahlia Malkhi, Alberto Sonnino, and Alexander Spiegelman

Jolteon and Ditto: Network-Adaptive Efficient Consensus with Asynchronous Fallback 296
Rati Gelashvili, Lefteris Kokoris-Kogias, Alberto Sonnino, Alexander Spiegelman, and Zhuolun Xiang

Quick Order Fairness 316
Christian Cachin, Jovana Mićić, Nathalie Steinhauer, and Luca Zanolini

Mostly Payment Networks

Analysis and Probing of Parallel Channels in the Lightning Network 337
Alex Biryukov, Gleb Naumenko, and Sergei Tikhomirov

HIDE & SEEK: Privacy-Preserving Rebalancing on Payment Channel Networks 358
Zeta Avarikioti, Krzysztof Pietrzak, Iosif Salem, Stefan Schmid, Samarth Tiwari, and Michelle Yeo

Short Paper: A Centrality Analysis of the Lightning Network 374
Philipp Zabka, Klaus-T. Foerster, Christian Decker, and Stefan Schmid

Resurrecting Address Clustering in Bitcoin 386
Malte Möser and Arvind Narayanan

Incentives

ABSNTF: Securitization and Repurchase Scheme for Non-Fungible Tokens Based on Game Theoretical Analysis	407
<i>Hongyin Chen, Yukun Cheng, Xiaotie Deng, Wenhan Huang, and Linxuan Rong</i>	
Decentralisation Conscious Players and System Reliability	426
<i>Sarah Azouvi and Alexander Hicks</i>	
Towards Overcoming the Undercutting Problem	444
<i>Tiantian Gong, Mohsen Minaei, Wenhai Sun, and Aniket Kate</i>	
Arbitrage Attack: Miners of the World, Unite!	464
<i>Yuheng Wang, Jiliang Li, Zhou Su, and Yuyi Wang</i>	
Suborn Channels: Incentives Against Timelock Bribes	488
<i>Zeta Avarikioti and Orfeas Stefanos Thyfronitis Litos</i>	
Sliding Window Challenge Process for Congestion Detection	512
<i>Ayelet Lotem, Sarah Azouvi, Patrick McCorry, and Aviv Zohar</i>	
Short Paper: On Game-Theoretically-Fair Leader Election	531
<i>Rati Gelashvili, Guy Goren, and Alexander Spiegelman</i>	

Not Proof of Work

The Availability-Accountability Dilemma and Its Resolution via Accountability Gadgets	541
<i>Joachim Neu, Ertem Nusret Tas, and David Tse</i>	
Three Attacks on Proof-of-Stake Ethereum	560
<i>Caspar Schwarz-Schilling, Joachim Neu, Barnabé Monnot, Aditya Asgaonkar, Ertem Nusret Tas, and David Tse</i>	
Permissionless Consensus in the Resource Model	577
<i>Benjamin Terner</i>	

Performance

Plumo: An Ultralight Blockchain Client	597
<i>Psi Vesely, Kobi Gurkan, Michael Straka, Ariel Gabizon, Philipp Jovanovic, Georgios Konstantopoulos, Asa Oines, Marek Olszewski, and Eran Tromer</i>	

SoK: Blockchain Light Clients	615
<i>Panagiotis Chatzigiannis, Foteini Baldimtsi, and Konstantinos Chalkias</i>	
Achieving Almost All Blockchain Functionalities with Polylogarithmic Storage	642
<i>Parikshit Hegde, Robert Streit, Yanni Georghiades, Chaya Ganesh, and Sriram Vishwanath</i>	
Measurements	
Short Paper: On the Claims of Weak Block Synchronization in Bitcoin	663
<i>Seungjin Baek, Hocheol Nam, Yongwoo Oh, Muoi Tran, and Min Suk Kang</i>	
India’s “Aadhaar” Biometric ID: Structure, Security, and Vulnerabilities	672
<i>Pratyush Ranjan Tiwari, Dhruv Agarwal, Prakhar Jain, Swagam Dasgupta, Preetha Datta, Vineet Reddy, and Debayan Gupta</i>	
Short Paper: What Peer Announcements Tell Us About the Size of the Bitcoin P2P Network	694
<i>Matthias Grundmann, Hedwig Amberg, Max Baumstark, and Hannes Hartenstein</i>	
An Empirical Study of Two Bitcoin Artifacts Through Deep Learning	705
<i>Richard Tindell, Alex Mitchell, Nathan Sprague, and Xunhua Wang</i>	
Author Index	725