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

Lecture Notes in Computer Science 13411

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

Springer

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

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	Talaia Labs, UK
Rafael Hirschfeld	Unipay Technologies, The Netherlands

Program Committee Chairs

Ittay Eyal	Technion, Israel
Juan Garay	Texas A&M University, USA

Steering Committee

Joseph Bonneau	New York University, 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

Program Committee

Ittai Abraham	VMware Research, Israel
Christian Badertscher	IOHK, Switzerland
Foteini Baldimtsi	George Mason University, USA
Jeremiah Blocki	Purdue University, USA
Rainer Böhme	University of Innsbruck, Austria
Joseph Bonneau	New York University, USA
Christian Cachin	University of Bern, Switzerland
L. Jean Camp	Indiana University, USA
Srdjan Capkun	ETH Zurich, Switzerland
Hubert Chan	University of Hong Kong, China
Jing Chen	Stony Brook University, USA
Michele Ciampi	University of Edinburgh, UK
Jeremy Clark	Concordia University, Canada
Vanesa Daza	Pompeu Fabra University, Spain
Stefan Dziembowski	University of Warsaw, Poland
Karim Eldefrawy	SRI International, USA
Matthias Fitzi	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	Nervos, USA
Yupeng Zhang	Texas A&M University, USA
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Vassilis Zikas	Purdue University, USA
Aviv Zohar	The Hebrew University, Israel

Contents

Tokenomics

MPC (Mostly)

Privacy

ZKP

Old-School Consensus

Mostly Payment Networks

Incentives

Not Proof of Work

Performance

Measurements