Lecture Notes in Computer Science **10322**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7410

Aggelos Kiayias (Ed.)

Financial Cryptography and Data Security

21st International Conference, FC 2017
Sliema, Malta, April 3–7, 2017
Revised Selected Papers

Springer

Editor
Aggelos Kiayias
University of Edinburgh
Edinburgh
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-70971-0 ISBN 978-3-319-70972-7 (eBook)
https://doi.org/10.1007/978-3-319-70972-7

Library of Congress Control Number: 2017959723

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

The 21st International Conference on Financial Cryptography and Data Security, FC 2017, was held during April 3–7, 2017, at the Palace Hotel in Malta.

We received 132 papers by the submission deadline for the conference which was November 14, 2016. Of these, seven were withdrawn and 35 were accepted – five as short papers and 30 as full papers – resulting in an acceptance rate of 26.5%. The present proceedings volume contains revised versions of all the papers presented at the conference.

The conference started with an invited talk by Silvio Micali, titled "ALGORAND: A New Public Ledger" and concluded with a panel titled "When Cash and Crypto Collide" with panelists Adam Back, Tiago Teles, and Tarah Wheeler, moderated by William Scannell.

The Program Committee consisted of 46 members spanning both industry and academia and covering all facets of financial cryptography. The review process took place over a period of two months and was double-blind. Each paper received at least three reviews; certain papers, including submissions by Program Committee members, received additional reviews. The Program Committee used the EasyChair system to organize the paper reviewing. The merits of each paper were discussed thoroughly and intensely in 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 made a substantial effort in improving the quality of accepted papers in the post-notification stage: 11 of the papers were conditionally accepted; each one was assigned a shepherd from the Program Committee who guided the authors in the preparation of the conference version.

A number of grateful acknowledgments are due. First and foremost, I would like to thank the authors of all submissions for contributing their work for peer review by the Program Committee. Their support of FC 2017 was the most important factor for the success of the conference. Second, I would like to thank the members of the Program Committee for investing a significant amount of their time in the review and discussion of the submitted papers. In addition to the Program Committee, 89 external reviewers were invited to contribute to the review process and I also thank them for their efforts. In total, 416 reviews were submitted, 3.328 on average per submission, with 76% of the reviews prepared by the Program Committee and the remainder by the external reviewers.

The conference also featured a poster session. I am grateful to the presenters of the posters for submitting their work and presenting it at the conference. The abstracts of the posters are included in this proceedings volume.

The general chairs of the conference were Adam Back and Rafael Hirschfeld. I would like to especially thank Rafael for his continued and tireless efforts to make FC a success over the years. A special thanks also goes to the board of directors of the International Financial Cryptography Association for their support and guidance.

Finally, I would like to thank Joe Bonneau for handling a submission with which I had a conflict of interest (it was authored by two PhD students of mine) completely outside to the reviewing system. I also thank the board of directors for allowing this submission to be considered.

Finally, I would like to thank all our sponsors this year, whose generous support was crucial in making the conference a success. In particular our platinum sponsors Blockstream, IOHK, and Thales, our gold sponsor Rohde and Schwarz, our silver sponsor *Journal of Cybersecurity* and our sponsor in kind WorldPay. For student support, I specifically thank the Office of Naval Research.

August 2017 Aggelos Kiayias

Organization

Program Committee

Masa Abe	NTT Laboratories
Ross Anderson	Cambridge University, UK
Diego Aranha	Institute of Computing, University of Campinas, Brazil
Frederik Armknecht	Universität Mannheim, Germany
Giuseppe Ateniese	Stevens Institute of Technology, USA
Foteini Baldimtsi	George Mason University, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Jeremiah Blocki	Purdue University, USA
Joe Bonneau	Stanford University, USA
Rainer Böhme	University of Innsbruck, Austria
Christian Cachin	IBM Research – Zurich, Switzerland
Jean Camp	Indiana University, USA
Srdjan Capkun	ETH Zurich, Switzerland
Jung Hee Cheon	Seoul National University, South Korea
Nicolas Christin	Carnegie Mellon University, USA
Jeremy Clark	Concordia University, Canada
Jean Paul Degabriele	RHUL
Dario Fiore	IMDEA Software Institute
Matt Green	Johns Hopkins, USA
Thomas Gross	University of Newcastle upon Tyne, UK
Jaap-Henk Hoepman	Radboud University Nijmegen, The Netherlands
Nicholas Hopper	University of Minnesota, USA
Kevin Huguenin	UNIL-HEC Lausanne, Switzerland
Stas Jarecki	University of California, Irvine, USA
Marc Joye	NXP Semiconductors
Stefan Katzenbeisser	TU Darmstadt, Germany
Aggelos Kiayias	University of Edinburgh, UK
Gäetan Leurent	Inria, France
Andrew Miller	University of Maryland, USA
Payman Mohassel	University of Calgary, Canada
Arvind Narayanan	Princeton, USA
Charalampos Papamanthou	University of Maryland, College Park, USA
Rafael Pass	Cornell University, USA
Bart Preneel	KU Leuven COSIC and iMinds, Belgium
Liz Quaglia	Royal Holloway, University of London, UK
Kazue Sako	NEC, Japan

Dominique Schröder	Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Douglas Stebila	McMaster University, Canada
Qiang Tang	Cornell University, USA
Kami Vaniea	The University of Edinburgh, UK
Serge Vaudenay	EPFL, Switzerland
Eric Wustrow	University of Colorado Boulder, USA
Bingsheng Zhang	Lancaster University, UK
Zhenfeng Zhang	Chinese Academy of Sciences, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Vasilis Zikas	ETH Zurich, Switzerland
Aviv Zohar	The Hebrew University of Jerusalem, Israel

Additional Reviewers

Abramova, Svetlana
Agrawal, Shashank
Alpar, Gergely
Balli, Fatih
Blazy, Olivier
Bogos, Sonia
Bos, Joppe
Bünz, Benedikt
Carter, Henry
Chaidos, Pyrros
Chepurnoy, Alex
Cherubin, Giovanni
Choi, Gwangbae
Costello, Craig
Davidson, Alex
Duong, Tuyet
Durak, F. Betül
Eom, Jieun
Fan, Lei
Fan, Xiong
Feher, Daniel
Frankel, Yair
Gervais, Arthur
Gordon, Dov
Großschädl, Johann
Han, Kyoohyung
Hansen, Torben
Heilman, Ethan
Hhan, Minki
Hils, Maximilian
Hiromasa, Ryo
Humbert, Mathias
Isshiki, Toshiyuki
Jeong, Jinhyuck
Karvelas, Nikolaos
Khovratovich, Dmitry
Kilinc, Handan
Kim, Duhyeong
Kim, Miran
Koide, Toshio
Kosba, Ahmed
Kostiainen, Kari
Köhler, Olaf Markus
Lacharité, Marie-Sarah
Laube, Stefan
Leontiadis, Iraklis
Li, Shuai
Li, Xinyu
Li, Zengpeng
Liu, Jian
Lu, Rongxing
Lu, Yun
Luhn, Sebastian
Malavolta, Giulio
Meyer, Maxime
Mori, Kengo
Naehrig, Michael
Ohkubo, Miyako

Olteanu, Alexandra-Mihaela
Pankova, Alisa
Peeters, Roel
Plût, Jérôme
Poettering, Bertram
Reinert, Manuel
Reuter, Christian A.
Riek, Markus
Ringers, Sietse
Ruffing, Tim
Schoettle, Pascal
Singelee, Dave
Son, Yongha
Teranishi, Isamu
Thyagarajan, Sri Aravinda Krishnan
Tikhomirov, Sergei
Tomida, Junichi
Udovenko, Aleksei
Vizár, Damian
Wang, Minqian
Wang, Qingju
Watson, Gaven
Weinstock, Avi
Woodage, Joanne
Yang, Kang
Young, Adam
Yu, Der-Yeuan
Zenner, Erik
Zhang, Lin
Zhang, Yupeng
Zindros, Dionysis

Contents