

## 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*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

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

Ian Goldberg · Tyler Moore (Eds.)

# Financial Cryptography and Data Security

23rd International Conference, FC 2019

Frigate Bay, St. Kitts and Nevis, February 18–22, 2019

Revised Selected Papers



Springer

*Editors*

Ian Goldberg  
Cheriton School of Computer Science  
University of Waterloo  
Waterloo, ON, Canada

Tyler Moore   
Tandy School of Computer Science  
University of Tulsa  
Tulsa, USA

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-32100-0              ISBN 978-3-030-32101-7 (eBook)  
<https://doi.org/10.1007/978-3-030-32101-7>

LNCS Sublibrary: SL4 – Security and Cryptology

© International Financial Cryptography Association 2019

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

FC 2019, the 23rd International Conference on Financial Cryptography and Data Security, was held February 18–22, 2019, at the St. Kitts Marriott Resort in Frigate Bay, St. Kitts and Nevis.

We received 178 paper submissions. Of these, 32 full papers and seven short papers were accepted, corresponding to a 21.9% acceptance rate. Revised papers appear in these proceedings.

The surge in interest in cryptocurrencies heralded by Bitcoin has been reflected in the composition of the program at FC for several years. Since 2014, a dedicated workshop, the Workshop on Bitcoin and Blockchain Research (BITCOIN), has been held in conjunction with FC. Given the quality and quantity of research appearing in this workshop, the International Financial Cryptography Association (IFCA) Steering Committee, in consultation with current and past program chairs of FC and the BITCOIN workshop, decided to integrate the BITCOIN workshop into the main FC conference as a new blockchain track.

This decision resulted in a high-quality and balanced program, with 20 papers in the new blockchain track and 19 papers in the non-blockchain track. The two tracks were held on alternating days: The blockchain track was Monday and Wednesday, and the non-blockchain track was Tuesday and Thursday. By not holding the tracks in parallel, all FC attendees could enjoy the entirety of the program. Neha Narula, Director of the MIT Digital Currency Initiative, gave an inspiring keynote entitled “Preventing Catastrophic Cryptocurrency Attacks.” Her talk highlighted some pressing and unique challenges of responsibly managing vulnerabilities affecting cryptocurrencies.

Overall, the program successfully realized the goal of creating a unified venue for blockchain papers, while keeping room for other topics that have long been part of FC. Feedback at the conference about the change was overwhelmingly positive. Therefore, we anticipate that this arrangement will continue in future editions of the conference.

We are grateful for the contributions of the 72 members of the Program Committee. Submissions had at least three reviews, or four in the case of a submission by a Program Committee member. An extensive online discussion phase was utilized to guide decisions. The Program Committee members provided thoughtful and constructive feedback to authors, which considerably strengthened the quality of the final papers appearing in this volume. Of the 39 accepted papers, 14 were shepherded by Program Committee members. We are especially thankful to the shepherds for their additional contributions. We also appreciate the reviews contributed by 59 external reviewers.

We would like to thank Rafael Hirschfeld for his unrivaled and continued dedication to FC, including his role serving as conference general chair. We also thank the IFCA directors and Steering Committee for their service.

Finally, we would like to thank the sponsors of the conference for their generous support: Research Institute, Blockstream, Chainanalysis, Kadena, Op Return, Quadrans Foundation, the Journal of Cybersecurity, and Worldpay.

We are excited to present the papers appearing in this volume. They represent some of the leading research in secure digital commerce, and we look forward to many more years of fruitful research presented at Financial Cryptography and Data Security.

July 2019

Ian Goldberg  
Tyler Moore

# Organization

## **Financial Cryptography and Data Security 2019 St. Kitts Marriott Resort, St. Kitts and Nevis February 18–22, 2019**

Organized by the  
*International Financial Cryptography Association*

In cooperation with the  
*International Association for Cryptologic Research*

### **General Chair**

Rafael Hirschfeld    Unipay, The Netherlands

### **Program Committee Chairs**

Ian Goldberg    University of Waterloo, Canada

Tyler Moore    The University of Tulsa, USA

### **Program Committee**

Shashank Agrawal	Visa Research, USA
Ross Anderson	Cambridge University, UK
Elli Androulaki	IBM Research - Zurich, Switzerland
Diego F. Aranha	Aarhus University, Denmark/University of Campinas, Brazil
Frederik Armknecht	University of Mannheim, Germany
Foteini Baldimtsi	George Mason University, USA
Iddo Bentov	Cornell Tech, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Jeremiah Blocki	Purdue University, USA
Rainer Böhme	Universität Innsbruck, Austria
Joseph Bonneau	New York University, USA
Alvaro A. Cardenas	University of Texas at Dallas, USA
Pern Hui Chia	Google, Switzerland
Sonia Chiasson	Carleton University, Canada
Nicolas Christin	Carnegie Mellon University, USA
Jeremy Clark	Concordia University, Canada
Gaby Dagher	Boise State University, USA
George Danezis	University College London, UK

Matteo Dell’Amico	Symantec Research Labs, France
Maria Dubovitskaya	DFINITY, Switzerland
Benjamin Edwards	IBM Research, USA
Tariq Elahi	University of Edinburgh, UK
William Enck	North Carolina State University, USA
Ittay Eyal	Technion, Israel
Antonio Faonio	IMDEA Software, Spain
Simone Fischer-Hübner	Karlstad University, Sweden
Bryan Ford	EPFL, Switzerland
Stephanie Forrest	Arizona State, USA
Juan Garay	Texas A&M University, USA
Christina Garman	Purdue University, USA
Matthew D. Green	Johns Hopkins University, USA
Rachel Greenstadt	New York University, USA
Jens Grossklags	Technical University of Munich, Germany
Feng Hao	Newcastle University, UK
Ethan Heilman	Boston University, USA
Urs Hengartner	University of Waterloo, Canada
Ryan Henry	University of Calgary, Canada
Nicholas Hopper	University of Minnesota, USA
Philipp Jovanovic	EPFL, Switzerland
Ghassan Karame	NEC Laboratories Europe, Germany
Aniket Kate	Purdue University, USA
Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
Florian Kerschbaum	University of Waterloo, Canada
Markulf Kohlweiss	University of Edinburgh, UK
Aron Laszka	University of Houston, USA
Helger Lipmaa	University of Tartu, Estonia
Wouter Lueks	EPFL, Switzerland
Kanta Matsuura	The University of Tokyo, Japan
Travis Mayberry	USA Naval Academy, USA
Patrick McCorry	King’s College London, UK
Catherine Meadows	USA Naval Research Laboratory, USA
Ian Miers	Cornell Tech, USA
Andrew Miller	University of Illinois at Urbana-Champaign, USA
Malte Maser	Princeton University, USA
Satoshi Obana	Hosei University, Japan
Olya Ohrimenko	Microsoft Research, UK
Simon Oya	University of Vigo, Spain
Elizabeth A. Quaglia	Royal Holloway, University of London, UK
Stefanie Roos	TU Delft, The Netherlands
Reihaneh Safavi-Naini	University of Calgary, Canada
Kazue Sako	NEC, Japan
Max Schuchard	University of Tennessee, USA
Abhi Shelat	Northeastern University, USA



Douglas Stebila	University of Waterloo, Canada
Luke Valenta	University of Pennsylvania, USA
Marie Vasek	University of New Mexico, USA
Marko Vukolic	IBM Research - Zurich, Switzerland
Eric Wustrow	University of Colorado Boulder, USA
Zhenfeng Zhang	Institute of Software, Chinese Academy of Sciences, China
Aviv Zohar	The Hebrew University, Israel

## Additional Reviewers

Kamalesh Acharya	Keisuke Kajigaya
Sefa Akca	Dimitris Karakostas
Miguel Ambrona	Patrik Keller
Dag Arne Osvik	Hamidreza Khoshakhlagh
Brian Arthur Shaft	Toomas Krips
Carsten Baum	Nikos Leonardos
Ritam Bhaumik	Peiyuan Liu
Chris Buckland	Angelique Loe
Matteo Campanelli	Antonio Marcedone
Panagiotis Chatzigiannis	Mohsen Minaei
Mo Chen	Mahsa Moosavi
Gareth Davies	Pedro Geraldo Morelli Rodrigues Alves
Angelo De Caro	Pratyay Mukherjee
Sergi Delgado Segura	Sanami Nakagawa
Pooja Dhomse	Alina Nesen
Edward Eaton	Bertram Poettering
Kasra EdalatNejad	Mastooreh Salajegheh
Kaoutar Elkhyaoui	Sajin Sasy
Batnyam Enkhtaivan	Janno Siim
Shayan Eskandari	Claudio Soriente
Prastudy Fauzi	Sergei Tikhomirov
Daniel Feher	Yiannis Tselekounis
Michael Frwis	Vesselin Velichkov
Benny Fuhry	Dhinakaran Vinayagamurthy
Matthias Hamann	Giuseppe Vitto
Ben Harsha	Tianhao Wang
Haruna Higo	Michal Zajac
Toshiyuki Isshiki	Santiago Zanella
Hkon Jacobsen	Samson Zhou
Benjamin Johnson	

# Contents

## Cryptocurrency Cryptanalysis

Biased Nonce Sense: Lattice Attacks Against Weak ECDSA Signatures in Cryptocurrencies . . . . .	3
<i>Joachim Breitner and Nadia Heninger</i>	

## Proofs of Stake

Snow White: Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake. . . . .	23
<i>Phil Daian, Rafael Pass, and Elaine Shi</i>	
Compounding of Wealth in Proof-of-Stake Cryptocurrencies . . . . .	42
<i>Giulia Fanti, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang</i>	
Short Paper: I Can't Believe It's Not Stake! Resource Exhaustion Attacks on PoS . . . . .	62
<i>Sanket Kanjalkar, Joseph Kuo, Yunqi Li, and Andrew Miller</i>	

## Measurement

Short Paper: An Exploration of Code Diversity in the Cryptocurrency Landscape . . . . .	73
<i>Pierre Reibel, Haaroon Yousaf, and Sarah Meiklejohn</i>	
Short Paper: An Empirical Analysis of Blockchain Forks in Bitcoin . . . . .	84
<i>Till Neudecker and Hannes Hartenstein</i>	
Detecting Token Systems on Ethereum . . . . .	93
<i>Michael Fröwis, Andreas Fuchs, and Rainer Böhme</i>	
Measuring Ethereum-Based ERC20 Token Networks. . . . .	113
<i>Friedhelm Victor and Bianca Katharina Lüders</i>	

## Traceability and How to Stop It

New Empirical Traceability Analysis of CryptoNote-Style Blockchains . . . . .	133
<i>Zuoxia Yu, Man Ho Au, Jiangshan Yu, Rupeng Yang, Qiuliang Xu, and Wang Fat Lau</i>	

Short Paper: An Empirical Analysis of Monero Cross-chain Traceability . . . .	150
<i>Abraham Hinteregger and Bernhard Haslhofer</i>	
PRCash: Fast, Private and Regulated Transactions for Digital Currencies . . .	158
<i>Karl Wüst, Kari Kostiainen, Vedran Čapkun, and Srdjan Čapkun</i>	
ZLiTE: Lightweight Clients for Shielded Zcash Transactions	
Using Trusted Execution . . . . .	179
<i>Karl Wüst, Sinisa Matetic, Moritz Schneider, Ian Miers, Kari Kostiainen, and Srdjan Čapkun</i>	
<b>Payment Protocol Security</b>	
Designed to Be Broken: A Reverse Engineering Study of the 3D Secure 2.0 Payment Protocol. . . . .	201
<i>Mohammed Aamir Ali and Aad van Moorsel</i>	
Short Paper: Making Contactless EMV Robust Against Rogue Readers	
Colluding with Relay Attackers . . . . .	222
<i>Tom Chothia, Ioana Boureanu, and Liqun Chen</i>	
Short Paper: How to Attack PSD2 Internet Banking . . . . .	234
<i>Vincent Haupert and Stephan Gabert</i>	
Your Money or Your Life—Modeling and Analyzing the Security	
of Electronic Payment in the UC Framework . . . . .	243
<i>Dirk Achenbach, Roland Gröll, Timon Hackenjos, Alexander Koch, Bernhard Löwe, Jeremias Mechler, Jörn Müller-Quade, and Jochen Rill</i>	
<b>Multiparty Protocols</b>	
Secure Trick-Taking Game Protocols: How to Play Online Spades	
with Cheaters . . . . .	265
<i>Xavier Bultel and Pascal Lafourcade</i>	
ROYALE: A Framework for Universally Composable Card Games	
with Financial Rewards and Penalties Enforcement . . . . .	282
<i>Bernardo David, Rafael Dowsley, and Mario Larangeira</i>	
Universally Verifiable MPC and IRV Ballot Counting . . . . .	301
<i>Kim Ramchen, Chris Culnane, Olivier Pereira, and Vanessa Teague</i>	
Synchronous Byzantine Agreement with Expected $O(1)$ Rounds,	
Expected $O(n^2)$ Communication, and Optimal Resilience . . . . .	320
<i>Ittai Abraham, Srinivas Devadas, Danny Dolev, Kartik Nayak, and Ling Ren</i>	

## Crypto Means Cryptography

Oblivious PRF on Committed Vector Inputs and Application to Deduplication of Encrypted Data. . . . .	337
<i>Jan Camenisch, Angelo De Caro, Esha Ghosh, and Alessandro Sorniotti</i>	
Adaptively Secure Constrained Pseudorandom Functions . . . . .	357
<i>Dennis Hofheinz, Akshay Kamath, Venkata Koppula, and Brent Waters</i>	
LARA: A Design Concept for Lattice-Based Encryption . . . . .	377
<i>Rachid El Bansarkhani</i>	
Short Paper: The Proof is in the Pudding: Proofs of Work for Solving Discrete Logarithms . . . . .	396
<i>Marcella Hastings, Nadia Heninger, and Eric Wustrow</i>	

## Getting Formal

Minimizing Trust in Hardware Wallets with Two Factor Signatures. . . . .	407
<i>Antonio Marcedone, Rafael Pass, and Abhi Shelat</i>	
A Formal Treatment of Hardware Wallets . . . . .	426
<i>Myrto Arapinis, Andriana Gkaniatsou, Dimitris Karakostas, and Angelos Kiayias</i>	
VeriSolid: Correct-by-Design Smart Contracts for Ethereum. . . . .	446
<i>Anastasia Mavridou, Aron Laszka, Emmanouela Stachtari, and Abhishek Dubey</i>	
Bitcoin Security Under Temporary Dishonest Majority . . . . .	466
<i>Georgia Avarikioti, Lukas Käppeli, Yuyi Wang, and Roger Wattenhofer</i>	

## Off-Chain Mechanisms and More Measurement

VAPOR: A Value-Centric Blockchain that is Scale-out, Decentralized, and Flexible by Design . . . . .	487
<i>Zhijie Ren and Zekeriya Erkin</i>	
Sprites and State Channels: Payment Networks that Go Faster Than Lightning. . . . .	508
<i>Andrew Miller, Iddo Bentov, Surya Bakshi, Ranjit Kumaresan, and Patrick McCorry</i>	
Echoes of the Past: Recovering Blockchain Metrics from Merged Mining . . .	527
<i>Nicholas Stifter, Philipp Schindler, Aljosha Judmayer, Alexei Zamyatin, Andreas Kern, and Edgar Weippl</i>	

<b>TxProbe: Discovering Bitcoin’s Network Topology Using Orphan Transactions . . . . .</b>	<b>550</b>
<i>Sergi Delgado-Segura, Surya Bakshi, Cristina Pérez-Solà, James Litton, Andrew Pachulski, Andrew Miller, and Bobby Bhattacharjee</i>	
<b>Fraud Detection and Game Theory</b>	
<b>Forecasting Suspicious Account Activity at Large-Scale Online Service Providers . . . . .</b>	<b>569</b>
<i>Hassan Halawa, Konstantin Beznosov, Baris Coskun, Meizhu Liu, and Matei Ripeanu</i>	
<b>Thinking Like a Fraudster: Detecting Fraudulent Transactions via Statistical Sequential Features . . . . .</b>	<b>588</b>
<i>Chen Jing, Cheng Wang, and Chungang Yan</i>	
<b>Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection . . .</b>	<b>605</b>
<i>Alex Sangers, Maran van Heesch, Thomas Attema, Thijs Veugen, Mark Wiggerman, Jan Veldsink, Oscar Bloemen, and Daniël Worm</i>	
<b>IoT Security, and Crypto Still Means Cryptography</b>	
<b>HEALED: HEaling &amp; Attestation for Low-End Embedded Devices. . . . .</b>	<b>627</b>
<i>Ahmad Ibrahim, Ahmad-Reza Sadeghi, and Gene Tsudik</i>	
<b>One-Time Programs Made Practical. . . . .</b>	<b>646</b>
<i>Lianying Zhao, Joseph I. Choi, Didem Demirag, Kevin R. B. Butler, Mohammad Mannan, Erman Ayday, and Jeremy Clark</i>	
<b>Statement Voting . . . . .</b>	<b>667</b>
<i>Bingsheng Zhang and Hong-Sheng Zhou</i>	
<b>Fast Authentication from Aggregate Signatures with Improved Security. . . . .</b>	<b>686</b>
<i>Muslum Ozgur Ozmen, Rouzbeh Behnia, and Attila A. Yavuz</i>	
<b>Author Index . . . . .</b>	<b>707</b>