

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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

Jeremy Clark · Sarah Meiklejohn
Peter Y.A. Ryan · Dan Wallach
Michael Brenner · Kurt Rohloff (Eds.)

Financial Cryptography and Data Security

FC 2016 International Workshops
BITCOIN, VOTING, and WAHC
Christ Church, Barbados, February 26, 2016
Revised Selected Papers

Editors

Jeremy Clark
Concordia University
Montreal, QC
Canada

Sarah Meiklejohn
University College London
London
UK

Peter Y.A. Ryan
Université du Luxembourg
Luxembourg
Luxembourg

Dan Wallach
Rice University
Houston, TX
USA

Michael Brenner
Leibniz Universität Hannover
Hannover
Germany

Kurt Rohloff
New Jersey Institute of Technology
Newark, NJ
USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-662-53356-7

ISBN 978-3-662-53357-4 (eBook)

DOI 10.1007/978-3-662-53357-4

Library of Congress Control Number: 2016949126

LNCS Sublibrary: SL4 – Security and Cryptology

© International Financial Cryptography Association 2016

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, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer-Verlag GmbH Berlin Heidelberg

BITCOIN 2016: Third Workshop on Bitcoin and Blockchain Research

We were pleased to once again hold a Bitcoin Workshop at Financial Cryptography and Data Security 2016. In the year leading up to our third workshop, many financial institutes—including banks, insurance companies, and security exchanges—began demonstrating interest in adapting Bitcoin’s blockchain data structure for applications relevant to them. To capitalize on this expanding focus, we tweaked the name of the workshop to include “Blockchain Research” that utilizes Bitcoin’s flagship component for broader or competing applications.

After completing the peer-review process, with gratitude to our outstanding Program Committee (listed herein), we selected ten papers for the workshop out of the 25 submissions we received. In addition to our program, we note that Financial Cryptography itself accepted six papers on Bitcoin; thus our joint conference remains a strong venue with a high concentration of new academic research into Bitcoin. Our programs contained a range of subjects but particular attention was paid to scalability issues in Bitcoin, as well as to the Ethereum platform.

We were pleased to have an insightful keynote presentation from Nathaniel Popper of the *New York Times* and author of *Digital Gold* touching on the history of Bitcoin and the people involved early in its development. We also had a rich security exposition of the Ethereum protocol and client by Gustav Simonsson of the Ethereum project. Finally, we witnessed a small sliver of Bitcoin history when Sean Bowe from zcash received the first zero-knowledge contingent payment live on the Bitcoin network from Gregory Maxwell in California.

We again extend our gratitude to our Program Committee for doing the hard work of selecting a strong set of papers for the workshop. Thanks in particular to Nicolas Christin for setting us up with a HotCRP server that made all of our lives easier, and to Joseph Bonneau for being the first PC member to complete all their reviews (his award is to be chair next year). We thank each of our invited speakers for taking the time to attend, interact, and give compelling talks. We thank all the attendees for their interest, questions, and interactions during the reception and breaks. We thank the organizers of Financial Cryptography, in particular the general chair, Ray Hirschfeld, for guiding us through the process and executing a flawless conference in a beautiful location. Finally we thank all of the sponsors of Financial Cryptography and, by extension, ourselves.

July 2016

Sarah Meiklejohn
Jeremy Clark

Program Committee

Gavin Andresen	MIT Media Lab, USA
Elli Androulaki	IBM Research Zurich, Switzerland
Foteini Baldimtsi	Boston University, USA
Iddo Bentov	Technion, Israel
Alex Biryukov	University of Luxembourg, Luxembourg
Joseph Bonneau	Stanford University and EFF, USA
Rainer Böhme	University of Innsbruck, Austria
Srdjan Capkun	ETH Zurich, Switzerland
Nicolas Christin	Carnegie Mellon University, USA
Christian Decker	ETH Zurich, Switzerland
Stefan Dziembowski	University of Warsaw, Poland
Ittay Eyal	Cornell University, USA
Christina Garman	Johns Hopkins University, USA
Matthew Green	Johns Hopkins University, USA
Jens Grossklags	Penn State University, USA
Feng Hao	Newcastle University, UK
Ethan Heilman	Boston University, USA
Garrick Hileman	London School of Economics, UK
Aquinas Hobor	National University of Singapore, Singapore
Aniket Kate	Purdue University, USA
Aggelos Kiayias	National Kapodistrian University of Athens, Greece
Gregory Maxwell	Blockstream/Bitcoin Core, USA
Tyler Moore	University of Tulsa, USA
Andrew Miller	University of Maryland, USA
Arvind Narayanan	Princeton University, USA
abhi shelat	University of Virginia, USA
Elaine Shi	Cornell University, USA
Aviv Zohar	The Hebrew University of Jerusalem, Israel

VOTING 2016: First Workshop on Advances in Secure Electronic Voting Schemes

In the summer of 2015 we were approached by the organizers of Financial Crypto with the suggestion to submit a proposal for a workshop on secure voting systems to contribute to marking the 20th anniversary of FC. We took up the invitation and the resulting proposal was duly accepted. This led to a rather shorter lead time for advertisement etc. than we would ideally have liked, but nonetheless the workshop was a success in terms of the number and quality of submissions, attendance, and the quality of presentations and the discussions.

Voting forms the foundation of democracy and as such voting systems constitute part of a democratic nation's critical infrastructure, albeit one that is only deployed periodically. Moves to use digital technologies in voting introduce a whole raft of new, poorly understood threats, especially when it comes to voting over the Internet. This has prompted the security and crypto communities to address the challenges of making voting technologies and systems that are really secure, principally ensuring that the outcome is demonstrably correct while guaranteeing the secrecy of votes.

We received 13 submissions, all of which had at least three reviews and several of which provoked lively debate among the reviewers. Six papers were accepted, leaving space for a keynote talk and a panel. We invited Glen Weyl of Microsoft Research New England and the University of Chicago to present his idea of quadratic voting and discuss the security aspects. The panel was organized by Mark Ryan of the University of Birmingham: "On the Possibility of Ever Deploying Internet-Based Voting," a discussion of the challenges and obstructions to developing secure and usable Internet voting systems.

We should like to thank the organizers of FC for inviting us to organize the workshop in association with the conference and for all their support throughout the process. We also thank all the authors who submitted papers but especially those who came to present the accepted papers. We also thank the PC for their sterling efforts, especially those who performed shepherd duties.

April 2015

Peter Y.A. Ryan
Dan Wallach

Program Committee

Michael Alvarez	California Institute of Technology, USA
Roberto Araujo	Universidade Federal do Pará, Brazil
Jeremy Clark	Concordia University, USA
Veronique Cortier	LORIA, CNRS, France
Jeremy Epstein	SRI, USA
Aleksander Essex	Western University
Kristian Gjosteen	Norwegian University of Science and Technology, Norway
Rajeev Gore	The Australian National University, Australia
Jeroen van de Graaf	Universidade Federal de Minas Gerais, Brazil
Rolf Haenni	Bern University of Applied Sciences, Switzerland
Reto König	Bern University of Applied Sciences, Switzerland
Steve Kremer	Inria Nancy, France
Robert Krimmer	Tallinn University of Technology, Estonia
Olivier Pereira	Universite Catholique de Louvain, Belgium
Ron L. Rivest	MIT, USA
Alon Rosen	IDC Herzliya, Israel
Mark Ryan	University of Birmingham, UK
Steve Schneider	University of Surrey, UK
Berry Schoenmakers	Eindhoven University of Technology, The Netherlands
Carsten Schuermann	IT University of Copenhagen, Denmark
Philip B. Stark	University of California, Berkeley, USA
Vanessa Teague	The University of Melbourne, Australia
Melanie Volkamer	TU Darmstadt, Germany
Poorvi Vora	The George Washington University, USA

WAHC 2016: 4th Workshop on Encrypted Computing and Applied Homomorphic Cryptography

Cloud hype and the recent leakage of private information show there is a demand for secure and practical computing technologies. The WAHC workshop addresses the challenge in safely outsourcing data processing onto remote computing resources by protecting programs and data even during processing. This allows users to outsource computation over confidential information independently from the trustworthiness or the security level of the remote delegate. The workshop serviced these research needs by collecting and bringing together some of the top researchers and practitioners from academia, government, and industry to present, discuss, and share the latest progress in the field relevant to real-world problems with practical approaches and solutions.

The workshop was uniformly attended by academia, government, and industry, with attendees both from prior years with experience in the domain and new attendees learning from the community. Specific encrypted computing technologies focused on homomorphic encryption and secure multiparty computation. The technologies and techniques discussed in this workshop are key to extending the range of applications that can be securely and practically outsourced.

Presentations and discussions at the workshop were of the high quality and deep insight we have come to expect from our community. Topics of conversation included insights and lessons learned from experience implementing encrypted computing schemes, and experience reports on applying these technologies. Special thanks to the invited speaker: Erman Ayday from Bilkent University, who shared experience from a recent encrypted computing projects applied to genetic testing.

This year we accepted demo papers for consideration. We had a strong inaugural demo paper presentation from Mamadou Diallo of SPAWAR System Center Pacific, who discussed applying homomorphic encryption technologies to support use cases for the US Navy.

All of the 11 submission contained unique and interesting results. Each was reviewed by at least three Program Committee members. While all the papers were of high quality, only five papers were accepted for the workshop. We thank the authors for their submissions, the members of the Program Committee for their effort, the workshop participants for attending, and the FC organizers for supporting us.

February 2016

Michael Brenner
Kurt Rohloff

Program Committee

Dan Bogdanov	Cybernetica, Estonia
Marten van Dijk	UConn, USA
Joan Feigenbaum	Yale, USA
Rosario Gennaro	CCNY, USA
Sergey Gorbunov	MIT, USA
Aggelos Kiayias	UConn, USA
Vlad Kolesnikov	Bell Labs, USA
Kim Laine	Microsoft, USA
Tancrède Lepoint	CryptoExperts, France
David Naccache	ENS, Paris, France
Michael Naehrig	Microsoft, USA
Pascal Paillier	CryptoExperts, France
Benny Pinkas	Bar-Ilan University, Israel
Yuriy Polyakov	NJIT, USA
Berk Sunar	WPI, USA
Mehdi Tibouchi	NTT, Japan
Yevgeniy Vahlis	Amazon, USA
Fré Vercauteren	KU Leuven, Belgium
Adrian Waller	Thales, UK

Contents

Third Workshop on Bitcoin and Blockchain Research, BITCOIN 2016

Stressing Out: Bitcoin “Stress Testing”	3
<i>Khaled Baqer, Danny Yuxing Huang, Damon McCoy, and Nicholas Weaver</i>	
Why Buy When You Can Rent? Bribery Attacks on Bitcoin-Style Consensus	19
<i>Joseph Bonneau</i>	
Automated Verification of Electrum Wallet	27
<i>Mathieu Turuani, Thomas Voegtlin, and Michael Rusinowitch</i>	
Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions	43
<i>Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg</i>	
Proofs of Proofs of Work with Sublinear Complexity	61
<i>Aggelos Kiayias, Nikolaos Lamprou, and Aikaterini-Panagiota Stouka</i>	
Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab	79
<i>Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Andrew Miller, and Elaine Shi</i>	
EthIKS: Using Ethereum to Audit a CONIKS Key Transparency Log	95
<i>Joseph Bonneau</i>	
On Scaling Decentralized Blockchains: (A Position Paper)	106
<i>Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer</i>	
Bitcoin Covenants	126
<i>Malte Möser, Ittay Eyal, and Emin Gün Sirer</i>	
Cryptocurrencies Without Proof of Work	142
<i>Iddo Bentov, Ariel Gabizon, and Alex Mizrahi</i>	

First Workshop on Secure Voting Systems, VOTING 2016

Coercion-Resistant Internet Voting with Everlasting Privacy	161
<i>Philipp Locher, Rolf Haenni, and Reto E. Koenig</i>	

Selene: Voting with Transparent Verifiability and Coercion-Mitigation	176
<i>Peter Y.A. Ryan, Peter B. Rønne, and Vincenzo Iovino</i>	
On the Possibility of Non-interactive E-Voting in the Public-Key Setting	193
<i>Rosario Giustolisi, Vincenzo Iovino, and Peter B. Rønne</i>	
Efficiency Comparison of Various Approaches in E-Voting Protocols	209
<i>Oksana Kulyk and Melanie Volkamer</i>	
Remote Electronic Voting Can Be Efficient, Verifiable and Coercion-Resistant	224
<i>Roberto Araújo, Amira Barki, Solenn Brunet, and Jacques Traoré</i>	
Universal Cast-as-Intended Verifiability	233
<i>Alex Escala, Sandra Guasch, Javier Herranz, and Paz Morillo</i>	
4th Workshop on Encrypted Computing and Applied Homomorphic Cryptography, WAHC 2016	
Hiding Access Patterns in Range Queries Using Private Information Retrieval and ORAM.	253
<i>Gamze Tillem, Ömer Mert Candan, Erkey Savaş, and Kamer Kaya</i>	
Optimizing MPC for Robust and Scalable Integer and Floating-Point Arithmetic	271
<i>Liisi Kerik, Peeter Laud, and Jaak Randmets</i>	
On-the-fly Homomorphic Batching/Unbatching.	288
<i>Yarkin Doröz, Gizem S. Çetin, and Berk Sunar</i>	
Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation.	302
<i>Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor</i>	
CallForFire: A Mission-Critical Cloud-Based Application Built Using the Nomad Framework	319
<i>Mamadou H. Diallo, Michael August, Roger Hallman, Megan Kline, Henry Au, and Vic Beach</i>	
Cryptographic Solutions for Genomic Privacy.	328
<i>Erman Ayday</i>	
Author Index	343