

*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>

Jens Grossklags · Bart Preneel (Eds.)

# Financial Cryptography and Data Security

20th International Conference, FC 2016  
Christ Church, Barbados, February 22–26, 2016  
Revised Selected Papers

*Editors*

Jens Grossklags  
Department of Informatics  
Technical University Munich  
Garching  
Germany

Bart Preneel  
Department of Electrical Engineering-ESAT  
KU Leuven  
Leuven  
Belgium

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-662-54969-8              ISBN 978-3-662-54970-4 (eBook)  
DOI 10.1007/978-3-662-54970-4

Library of Congress Control Number: 2017940629

LNCS Sublibrary: SL4 – Security and Cryptology

© International Financial Cryptography Association 2017

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer-Verlag GmbH Germany  
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

# Preface

FC 2016, the 20th International Conference on Financial Cryptography and Data Security, was held during February 22–26, 2016, at the Accra Beach Hotel and Spa Barbados. This edition was a special 20th anniversary edition featuring some extra items in the program.

We received 137 paper submissions, out of which 36 were accepted, nine as short papers and 27 as full papers, resulting in an acceptance rate of 26%. These proceedings contain revised versions of all the papers. The 20th anniversary keynotes were delivered by privacy pioneer David Chaum, who spoke on “Privategrity” and Turing award winner Adi Shamir who shared with the audience his perspective on “The Past, Present and Future of Financial Cryptography.” The program was complemented by a special anniversary panel entitled “The Promises and Pitfalls of Distributed Consensus Systems: From Contract Signing to Cryptocurrencies.”

The Program Committee consisted of 49 members with diverse backgrounds and broad research interests. The review process was double-blind. Each paper received at least three reviews; for submissions by Program Committee members this was increased to four. During the discussion phase, additional reviews were solicited when necessary. An intensive discussion was held to clarify issues and to converge towards decisions. The selection of the program was challenging; in the end some high-quality papers had to be rejected due to lack of space.

We would like to sincerely thank the authors of all submissions for contributing high-quality submissions and giving us the opportunity to compile a strong and diverse program.

Special thanks go to the Program Committee members; we value their hard work and dedication to write careful and detailed reviews and to engage in interesting discussions. A few Program Committee members, whom we asked to serve as shepherds, spent additional time in order to help the authors improve their works. More than 60 external reviewers contributed to the review process; we would like to thank them for their efforts.

We are greatly indebted to Rafael Hirschfeld, the conference general chair, for his tireless efforts to make the conference a success. We also would like to thank the anniversary chairs, Sven Dietrich and Ahmad Sadeghi. Special thanks go the board of directors of the International Financial Cryptography Association for their support and advice.

Finally, we would like to thank the Office of Naval Research Global (ONR Global), bitt, the CROSSING project at TU Darmstadt, Rohde & Schwartz, AtenCoin, Gemini, Google, the *Journal of Cybersecurity*, KOBIL, SAP, KPMG, Worldpay, and the NSF for their generous support of the conference.

We hope that the papers in this volume prove valuable for your research and professional activities and that Financial Cryptography and Data Security will continue to play its unique role in bringing together researchers and practitioners in the area of secure digital commerce.

February 2017

Jens Grossklags  
Bart Preneel

**FC 2016**

**Financial Cryptography and Data Security 2016**  
**Accra Beach Hotel and Spa, Barbados**  
**February 22–26, 2016**

Organized by the  
*International Financial Cryptography Association*

In cooperation with the  
*International Association for Cryptologic Research*

**General Chair**

Rafael Hirschfeld                      Unipay, The Netherlands

**Anniversary Chairs**

Sven Dietrich                      City University of New York, USA  
Ahmad Sadeghi                      TU Darmstadt, Germany

**Program Chairs**

Jens Grossklags                      TU Munich, Germany  
Bart Preneel                      KU Leuven, Belgium

**Program Committee**

Masayuki Abe	NTT Laboratories, Japan
Alessandro Acquisti	Carnegie Mellon University, USA
Ross Anderson	Cambridge University, UK
Elli Androulaki	IBM Research Zurich, Switzerland
N. Asokan	Aalto University, Finland
Paulo Barreto	University of Sao Paulo, Brazil
Steven Bellovin	Columbia University, USA
Daniel Bernstein	University of Illinois at Chicago, USA
Rainer Böhme	University of Innsbruck, Austria
Alvaro Cardenas	University of Texas at Dallas, USA
Jeremy Clark	Concordia University, USA
Nicolas Courtois	University College London, UK
George Danezis	University College London, UK
Serge Egelman	UC Berkeley, USA

Seda Gürses	NYU, USA
Feng Hao	Newcastle University, UK
Thorsten Holz	Ruhr University Bochum, Germany
Trent Jaeger	The Pennsylvania State University, USA
Markus Jakobsson	Qualcomm, USA
Benjamin Johnson	Carnegie Mellon University, USA
Aniket Kate	Purdue University, USA
Florian Kerschbaum	SAP, Germany
Aggelos Kiayias	National and Kapodistrian University of Athens, Greece
Bart Knijnenburg	Clemson University, USA
Markulf Kohlweiss	Microsoft Research, UK
Aron Laszka	UC Berkeley, USA
Anja Lehmann	IBM Research Zurich, Switzerland
Arjen Lenstra	EPFL, Switzerland
Patrick Loiseau	EURECOM, France
Travis Mayberry	US Naval Academy, USA
Catherine Meadows	Naval Research Laboratory, USA
Sarah Meiklejohn	University College London, UK
Tyler Moore	University of Tulsa, USA
Steven Murdoch	University College London, UK
Tatsuaki Okamoto	NTT Laboratories, Japan
Kenneth Paterson	Royal Holloway, University of London, UK
Roberto Perdisci	University of Georgia, USA
Avi Rubin	Johns Hopkins University, USA
Ahmad Sadeghi	TU Darmstadt, Germany
Rei Safavi-Naini	University of Calgary, Canada
Nigel Smart	University of Bristol, UK
Jessica Staddon	Google, USA
Carmela Troncoso	Gradiant, Spain
Damien Vergnaud	École Normale Supérieure, France
Nicholas Weaver	International Computer Science Institute, USA
Xinyu Xing	The Pennsylvania State University, USA
Moti Yung	Google and Columbia University, USA

## Additional Reviewers

Svetlana Abramova	Zekeriya Erkin	Vijay Kamble
Enrique Argones	Sadegh Farhang	Gabe Kaptchuk
Ero Balsa	Ben Fisch	Carmen Kempka
Erik-Oliver Blass	Oana Goga	Sheharbano Khattak
Matthias Carnein	Steven Goldfeder	Ryo Kikuchi
Joseph Carrigan	Marian Harbach	Markus Krause
Alex Davidson	Heqing Huang	Junichiro Kume
Angelo De Caro	Brittany Johnson	Stefan Laube



Sebastian Luhn  
Caitlin Lustig  
Samuel Marchal  
Paul Martin  
Patrick Mccorry  
Maryam Mehrnezhad  
Aastha Mehta  
Tarik Moataz  
Malte Möser  
Thomas Nyman  
Miyako Ohkubo  
Olga Ohrimenko  
Melek Önen  
Cristina Onete  
Simon Oya

Giorgos Panagiotakos  
Goutam Paul  
Andrew Paverd  
Yu Pu  
Elizabeth Anne Quaglia  
Markus Riek  
Michael Rushanan  
Katerina Samari  
Daniel Sanchez  
Luiza Sayfullina  
Pascal Schoettle  
Siamak F. Shahandashti  
Kumar Sharad  
Karthik Sheshadri  
Brian Sniffen

Koutarou Suzuki  
Syed Taha  
Sandeep Tamrakar  
Qiang Tang  
Yiannis Tselekounis  
Marie Vasek  
David Wagner  
Brecht Wyseur  
Yi Xu  
Thomas Zacharias  
Greg Zaverucna  
Bingsheng Zhang  
Dionysis Zindros

# Contents

## Fraud and Deception

Understanding Craigslist Rental Scams . . . . .	3
<i>Youngsam Park, Damon McCoy, and Elaine Shi</i>	
Graph Analytics for Real-Time Scoring of Cross-Channel Transactional Fraud . . . . .	22
<i>Ian Molloy, Suresh Chari, Ulrich Finkler, Mark Wiggerman, Coen Jonker, Ted Habeck, Youngja Park, Frank Jordens, and Ron van Schaik</i>	
Android UI Deception Revisited: Attacks and Defenses . . . . .	41
<i>Earlence Fernandes, Qi Alfred Chen, Justin Paupore, Georg Essl, J. Alex Halderman, Z. Morley Mao, and Atul Prakash</i>	
Introducing Reputation Systems to the Economics of Outsourcing Computations to Rational Workers . . . . .	60
<i>Jassim Aljuraidan, Lujo Bauer, Michael K. Reiter, and Matthias Beckerle</i>	

## Payments, Auctions, and e-Voting

Accountable Privacy for Decentralized Anonymous Payments. . . . .	81
<i>Christina Garman, Matthew Green, and Ian Miers</i>	
Private eCash in Practice (Short Paper) . . . . .	99
<i>Amira Barki, Solenn Brunet, Nicolas Desmoulins, Sébastien Gambs, Saïd Gharout, and Jacques Traoré</i>	
Practically Efficient Secure Single-Commodity Multi-market Auctions. . . . .	110
<i>Abdelrahman Aly and Mathieu Van Vyve</i>	
How to Challenge and Cast Your e-Vote . . . . .	130
<i>Sandra Guasch and Paz Morillo</i>	

## Multiparty Computation

VD-PSI: Verifiable Delegated Private Set Intersection on Outsourced Private Datasets . . . . .	149
<i>Aydin Abadi, Sotirios Terzis, and Changyu Dong</i>	

Confidential Benchmarking Based on Multiparty Computation . . . . .	169
<i>Ivan Damgård, Kasper Damgård, Kurt Nielsen, Peter Sebastian Nordholt, and Tomas Toft</i>	
Efficiently Making Secure Two-Party Computation Fair. . . . .	188
<i>Handan Kılınç and Alptekin Küpçü</i>	
Fast Optimistically Fair Cut-and-Choose 2PC . . . . .	208
<i>Alptekin Küpçü and Payman Mohassel</i>	
<b>Mobile Malware</b>	
CuriousDroid: Automated User Interface Interaction for Android Application Analysis Sandboxes . . . . .	231
<i>Patrick Carter, Collin Mulliner, Martina Lindorfer, William Robertson, and Engin Kirda</i>	
DroydSeuss: A Mobile Banking Trojan Tracker (Short Paper) . . . . .	250
<i>Alberto Coletta, Victor van der Veen, and Federico Maggi</i>	
DroidAuditor: Forensic Analysis of Application-Layer Privilege Escalation Attacks on Android (Short Paper) . . . . .	260
<i>Stephan Heuser, Marco Negro, Praveen Kumar Pendyala, and Ahmad-Reza Sadeghi</i>	
<b>Social Interaction and Policy</b>	
Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper). . . . .	271
<i>Tristan Caulfield, Christos Ioannidis, and David Pym</i>	
<b>Cryptanalysis</b>	
Failures of Security APIs: A New Case . . . . .	283
<i>Abdalnaser Algwil and Jeff Yan</i>	
Explicit Optimal Binary Pebbling for One-Way Hash Chain Reversal . . . . .	299
<i>Berry Schoenmakers</i>	
Factoring as a Service . . . . .	321
<i>Luke Valenta, Shaanan Cohneney, Alex Liao, Joshua Fried, Satya Bodduluri, and Nadia Heninger</i>	
The Self-blindable U-Prove Scheme from FC'14 Is Forgeable (Short Paper) . . . . .	339
<i>Eric Verheul, Sietse Ringers, and Jaap-Henk Hoepman</i>	

A Sound for a Sound: Mitigating Acoustic Side Channel Attacks on Password Keystrokes with Active Sounds . . . . .	346
<i>S. Abhishek Anand and Nitesh Saxena</i>	

### **Surveillance and Anonymity**

Leaky Birds: Exploiting Mobile Application Traffic for Surveillance . . . . .	367
<i>Eline Vanrykel, Gunes Acar, Michael Herrmann, and Claudia Diaz</i>	
Footprint Scheduling for Dining-Cryptographer Networks . . . . .	385
<i>Anna Krasnova, Moritz Neikes, and Peter Schwabe</i>	

### **Web Security and Data Privacy**

How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication . . . . .	405
<i>Radhesh Krishnan Konoth, Victor van der Veen, and Herbert Bos</i>	
Security Keys: Practical Cryptographic Second Factors for the Modern Web . . . . .	422
<i>Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas</i>	
Include Me Out: In-Browser Detection of Malicious Third-Party Content Inclusions. . . . .	441
<i>Sajjad Arshad, Amin Kharraz, and William Robertson</i>	
A Sensitivity-Adaptive $\rho$ -Uncertainty Model for Set-Valued Data . . . . .	460
<i>Liuhua Chen, Shenghai Zhong, Li-e Wang, and Xianxian Li</i>	

### **Bitcoin Mining**

Incentive Compatibility of Bitcoin Mining Pool Reward Functions . . . . .	477
<i>Okke Schrijvers, Joseph Bonneau, Dan Boneh, and Tim Roughgarden</i>	
When Cryptocurrencies Mine Their Own Business . . . . .	499
<i>Jason Teutsch, Sanjay Jain, and Prateek Saxena</i>	
Optimal Selfish Mining Strategies in Bitcoin . . . . .	515
<i>Ayelet Sapirshstein, Yonatan Sompolinsky, and Aviv Zohar</i>	

### **Cryptographic Protocols**

A Short Paper on Blind Signatures from Knowledge Assumptions . . . . .	535
<i>Lucjan Hanzlik and Kamil Kluczniak</i>	

KBID: Kerberos Bracelet Identification (Short Paper) . . . . . 544  
*Joseph Carrigan, Paul Martin, and Michael Rushanan*

**Payment Use and Abuse**

The Other Side of the Coin: User Experiences with Bitcoin Security  
and Privacy . . . . . 555  
*Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer,  
and Edgar Weippl*

Refund Attacks on Bitcoin’s Payment Protocol . . . . . 581  
*Patrick McCorry, Siamak F. Shahandashti, and Feng Hao*

Are Payment Card Contracts Unfair? (Short Paper) . . . . . 600  
*Steven J. Murdoch, Ingolf Becker, Ruba Abu-Salma, Ross Anderson,  
Nicholas Bohm, Alice Hutchings, M. Angela Sasse,  
and Gianluca Stringhini*

The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin  
Brain Wallets . . . . . 609  
*Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith,  
and Tyler Moore*

**Author Index** . . . . . 619