

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>

Aggelos Kiayias (Ed.)

Financial Cryptography and Data Security

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

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

© International Financial Cryptography Association 2017, corrected publication 2023

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

Privacy and Identity Management

An Efficient Self-blindable Attribute-Based Credential Scheme	3
<i>Sietse Ringers, Eric Verheul, and Jaap-Henk Hoepman</i>	
Real Hidden Identity-Based Signatures	21
<i>Sherman S. M. Chow, Haibin Zhang, and Tao Zhang</i>	
BehavioCog: An Observation Resistant Authentication Scheme.	39
<i>Jagmohan Chauhan, Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Jonathan Chan, and Mohamed Ali Kaafar</i>	
Updatable Tokenization: Formal Definitions and Provably Secure Constructions	59
<i>Christian Cachin, Jan Camenisch, Eduarda Freire-Stögbuchner, and Anja Lehmann</i>	

Privacy and Data Processing

SecGDB: Graph Encryption for Exact Shortest Distance Queries with Efficient Updates	79
<i>Qian Wang, Kui Ren, Minxin Du, Qi Li, and Aziz Mohaisen</i>	
Outsourcing Medical Dataset Analysis: A Possible Solution	98
<i>Gabriel Kaptchuk, Matthew Green, and Aviel Rubin</i>	
Homomorphic Proxy Re-Authenticators and Applications to Verifiable Multi-User Data Aggregation	124
<i>David Derler, Sebastian Ramacher, and Daniel Slamanig</i>	

Cryptographic Primitives and API's

A Provably Secure PKCS#11 Configuration Without Authenticated Attributes.	145
<i>Ryan Stanley-Oakes</i>	
A Post-quantum Digital Signature Scheme Based on Supersingular Isogenies	163
<i>Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Jao, and Vladimir Soukharev</i>	

Optimally Sound Sigma Protocols Under DCRA.	182
<i>Helger Lipmaa</i>	

Economically Optimal Variable Tag Length Message Authentication.	204
<i>Reihaneh Safavi-Naini, Viliam Lisý, and Yvo Desmedt</i>	

Vulnerabilities and Exploits

PEEP: Passively Eavesdropping Private Input via Brainwave Signals.	227
<i>Ajaya Neupane, Md. Lutfor Rahman, and Nitesh Saxena</i>	

Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript.	247
<i>Michael Schwarz, Clémentine Maurice, Daniel Gruss, and Stefan Mangard</i>	

Attacks on Secure Logging Schemes.	268
<i>Gunnar Hartung</i>	

Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS.	285
<i>Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic</i>	

Short Paper: A Longitudinal Study of Financial Apps in the Google Play Store.	302
<i>Vincent F. Taylor and Ivan Martinovic</i>	

Short Paper: Addressing Sophisticated Email Attacks.	310
<i>Markus Jakobsson</i>	

Blockchain Technology

Escrow Protocols for Cryptocurrencies: How to Buy Physical Goods Using Bitcoin.	321
<i>Steven Goldfeder, Joseph Bonneau, Rosario Gennaro, and Arvind Narayanan</i>	

Trust Is Risk: A Decentralized Financial Trust Platform.	340
<i>Orfeas Stefanos Thyfronitis Litos and Dionysis Zindros</i>	

A Smart Contract for Boardroom Voting with Maximum Voter Privacy.	357
<i>Patrick McCorry, Siamak F. Shahandashti, and Feng Hao</i>	

Improving Authenticated Dynamic Dictionaries, with Applications to Cryptocurrencies	376
<i>Leonid Reyzin, Dmitry Meshkov, Alexander Chepurnoy, and Sasha Ivanov</i>	

Short Paper: Service-Oriented Sharding for Blockchains.	393
<i>Adem Efe Gencer, Robbert van Renesse, and Emin Gün Sirer</i>	

Security of Internet Protocols

The Security of NTP’s Datagram Protocol	405
<i>Aanchal Malhotra, Matthew Van Gundy, Mayank Varia, Haydn Kennedy, Jonathan Gardner, and Sharon Goldberg</i>	

Short Paper: On Deployment of DNS-Based Security Enhancements	424
<i>Pawel Szalachowski and Adrian Perrig</i>	

Blind Signatures

A Practical Multivariate Blind Signature Scheme	437
<i>Albrecht Petzoldt, Alan Szepieniec, and Mohamed Saied Emam Mohamed</i>	

Efficient Round-Optimal Blind Signatures in the Standard Model	455
<i>Essam Ghadafi</i>	

Searching and Processing Private Data

Secure Multiparty Computation from SGX.	477
<i>Raad Bahmani, Manuel Barbosa, Ferdinand Brasser, Bernardo Portela, Ahmad-Reza Sadeghi, Guillaume Scerri, and Bogdan Warinschi</i>	

Efficient No-dictionary Verifiable Searchable Symmetric Encryption	498
<i>Wakaha Ogata and Kaoru Kurosawa</i>	

Faster Homomorphic Evaluation of Discrete Fourier Transforms	517
<i>Anamaria Costache, Nigel P. Smart, and Srinivas Vivek</i>	

Secure Channel Protocols

Short Paper: TLS Ecosystems in Networked Devices vs. Web Servers.	533
<i>Nayanamana Samarasinghe and Mohammad Mannan</i>	

Unilaterally-Authenticated Key Exchange.	542
<i>Yevgeniy Dodis and Dario Fiore</i>	

Formal Modeling and Verification for Domain Validation and ACME	561
<i>Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Nadim Kobeissi</i>	

Why Banker Bob (Still) Can't Get TLS Right: A Security Analysis of TLS in Leading UK Banking Apps	579
<i>Tom Chothia, Flavio D. Garcia, Chris Heppell, and Chris McMahon Stone</i>	

Privacy in Data Storage and Retrieval

Lavinia: An Audit-Payment Protocol for Censorship-Resistant Storage	601
<i>Cecylia Bocovich, John A. Doucette, and Ian Goldberg</i>	

A Simpler Rate-Optimal CPIR Protocol	621
<i>Helger Lipmaa and Kateryna Pavlyk</i>	

Correction to: Why Banker Bob (Still) Can't Get TLS Right: A Security Analysis of TLS in Leading UK Banking Apps	C1
<i>Tom Chothia, Flavio D. Garcia, Chris Heppell, and Chris McMahon Stone</i>	

Poster Papers

Accountability and Integrity for Data Management Using Blockchains.	641
<i>Anirban Basu, Joshua Jeason Daniel, Sushmita Ruj, Mohammad Shahriar Rahman, Theo Dimitrakos, and Shinsaku Kiyomoto</i>	

The Amount as a Predictor of Transaction Fraud.	643
<i>Niek J. Bouman and Martha E. Nikolaou</i>	

Σ -State Authentication Language, an Alternative to Bitcoin Script.	644
<i>Alexander Chepurnoy</i>	

Broker-Mediated Trade Finance with Blockchains.	646
<i>Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto</i>	

OpenTimestamps: Securing Software Updates Using the Bitcoin Blockchain	647
<i>Peter Todd and Harry Halpin</i>	

Author Index	649
-------------------------------	-----