

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, Zürich, 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>

Vassilis Zikas · Roberto De Prisco (Eds.)

Security and Cryptography for Networks

10th International Conference, SCN 2016
Amalfi, Italy, August 31 – September 2, 2016
Proceedings

Editors

Vassilis Zikas
Rensselaer Polytechnic Institute
Troy, NY
USA

Roberto De Prisco
University of Salerno
Fisciano
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-44617-2 ISBN 978-3-319-44618-9 (eBook)
DOI 10.1007/978-3-319-44618-9

Library of Congress Control Number: 2016947481

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 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 International Publishing AG Switzerland

Preface

The 10th Conference on Security and Cryptography for Networks (SCN 2016) was held in Amalfi, Italy, from August 31 to September 2, 2016. The conference has traditionally been held in Amalfi, with the exception of the fifth edition that was held in the nearby Maiori. The first three editions of the conference were held in 1996, 1999, and 2002. Since 2002, the conference has been held biannually.

Modern communication is achieved mostly through the use of computer networks. Computer networks bring many advantages, such as easy access to information and fast communication. However guaranteeing security of distributed transactions is a challenging task. The SCN conference is an international meeting whose goal is to bring together researchers, practitioners, and developers interested in the security of communication networks, in order to foster cooperation, facilitate exchange of ideas, and disseminate research results.

The conference received 67 submissions in a broad range of cryptography and security areas. The Program Committee has selected, among the many high-quality submissions, 30 technical papers for publication in these proceedings. The selection took into account quality, originality, and relevance to the conference's scope. In addition, this year we received a crypto-lyrics paper titled "Zero-Knowledge Made Easy So It Won't Make You Dizzy" that the Program Committee found to be of great quality and therefore decided to grant it a special slot in the proceedings. It is our hope that this can motivate more of these high-quality creative and entertaining types of submissions in the future.

The international Program Committee (PC) consisted of 32 members who are top experts in the conference fields. At least three PC members reviewed each submitted paper, while submissions co-authored by a PC member were subjected to the more stringent evaluation of four PC members. In addition to the PC members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this knowledgeable and energetic team of experts, and are deeply grateful to all of them for their hard and thorough work, which included a very active discussion phase. Special thanks to Jeremiah Blocki, Alessandra Scafuro, Susumu Kiyoshima, Dimitris Papadopoulos, Juan Garay, and Sanjam Garg, for their extra work as shepherds.

The program was further enriched by the invited talks of Aggelos Kiayias (University of Edinburgh, UK) and Rafael Pass (Cornell University and Cornell NYC Tech, USA).

SCN 2016 was organized in cooperation with the International Association for Cryptologic Research (IACR). The paper submission, review, and discussion processes were effectively and efficiently made possible by the IACR Web-Submission-and-Review software, written by Shai Halevi. Many thanks to Shai for his assistance with the system's various features and constant availability.

We thank all the authors who submitted papers to this conference, the Organizing Committee members, colleagues, and student helpers for their valuable time and effort, and all the conference attendees who made this event truly intellectually stimulating through their active participation.

We finally thank the Dipartimento di Informatica of the Università degli Studi di Salerno, InfoCert, and the Università degli Studi di Salerno for their financial support.

September 2016

Vassilis Zikas
Roberto De Prisco

SCN 2016

The 10th Conference on Security and Cryptography for Networks

Amalfi, Italy
August 31 to September 2, 2016

Organized by
Dipartimento di Informatica
Università di Salerno

In Cooperation with
The International Association for Cryptologic Research (IACR)

Program Chair

Vassilis Zikas Rensselaer Polytechnic Institute (RPI), USA

General Chair

Roberto De Prisco Università di Salerno, Italy

Organizing Committee

Carlo Blundo Università di Salerno, Italy
Aniello Castiglione Università di Salerno, Italy
Luigi Catuogno Università di Salerno, Italy
Paolo D'Arco Università di Salerno, Italy

Steering Committee

Alfredo De Santis Università di Salerno, Italy
Ueli Maurer ETH Zürich, Switzerland
Rafail Ostrovsky University of California - Los Angeles, USA
Giuseppe Persiano Università di Salerno, Italy
Jacques Stern ENS, France
Douglas Stinson University of Waterloo, Canada
Gene Tsudik University of California - Irvine, USA
Moti Yung Snapchat and Columbia University, USA

Program Committee

Divesh Aggarwal EPFL, Switzerland
Shweta Agrawal Indian Institute of Technology, India
Joël Alwen IST, Austria

Gilad Asharov	The Hebrew University of Jerusalem, Israel
Foteini Baldimtsi	Boston University, USA and University of Athens, Greece
Jeremiah Blocki	Microsoft Research, USA
David Cash	Rutgers University, USA
Nishanth Chandran	Microsoft Research, India
Karim El Defrawy	HRL Labs, USA
Sebastian Faust	Ruhr-Universität Bochum, Germany
Juan Garay	Yahoo Labs, USA
Sanjam Garg	UC Berkeley, USA
Shafi Goldwasser	MIT, USA
Stanislaw Jarecki	UC Irvine, USA
Iordanis Kerenidis	University of Paris Diderot 7, France
Ranjit Kumaresan	MIT, USA
Steve Lu	Stealth Software Technologies Inc., USA
Ueli Maurer	ETH Zurich, Switzerland
Charalampos Papamanthou	University of Maryland, USA
Anat Paskin-Cherniavsky	Ariel University, Israel
Rafael Pass	Cornell University and Cornell NYC Tech., USA
Kenny Paterson	Royal Holloway, University of London, UK
Christian Rechberger	DTU, Denmark
Raphael Reischuk	ETH Zurich, Switzerland
Alessandra Scafuro	Boston University and Northeastern University, USA
Peter Schwabe	Radboud University, The Netherlands
Damien Stehl	ENS de Lyon, France
Marc Stevens	CWI, The Netherlands
Vanessa Teague	University of Melbourne, Australia
Stefano Tessaro	UC Santa Barbara, USA
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Vassilis Zikas	RPI, USA

External Reviewers

Shashank Agrawal	Chris Culnane	Carmit Hazay
Daniel Apon	Joan Daemen	Brett Hemenway
Christian Badertscher	Wei Dai	Aayush Jain
Saikrishna Badrinarayan	Angelo De Caro	Charanjit Jutla
Iddo Bentov	Akshay Degwekar	Chethan Kamath
Alexandra Berkoff	David Derler	Handan Kilinc
Florian Bourse	Julien Devigne	Susumu Kiyoshima
Christina Brzuska	Lo Ducas	Karen Klein
Jie Chen	Lisa Eckey	Ahmed Kosba
Alain Couvreur	Xiong Fan	Luke Kowalczyk

Eyal Kushilevitz
 Kim Laine
 Joshua Lampkins
 Adeline Langlois
 Enrique Larraia
 Tancrede Lepoint
 Satyanarayana Lokam
 Bernardo Machado David
 Rusydi Makarim
 Antonio Marcedone
 Nico Marcel Döttling
 Alexander May
 Sebastian Meiser
 Peihan Miao
 Sonia Mihaela Bogos
 Katerina Mitrokotsa
 Pratyay Mukherjee

Kartik Nayak
 Dimitris Papadopoulos
 Kostas Papagiannopoulos
 Alain Passelgue
 Antigoni Polychroniadou
 Ishaan Preet Singh
 Srinivasan Raghuraman
 Somindu Ramanna
 Kim Ramchen
 Vanishree Rao
 Tom Ristenpart
 Abhi shelat
 Katerina Samari
 Daniel Slamanig
 Nigel Smart
 Pratik Soni
 Akshayaram Srinivasan

Douglas Stebila
 Bjoern Tackmann
 Qiang Tang
 Alin Tomescu
 Roberto Trifiletti
 Daniel Tschudi
 Daniele Venturi
 Frederik Vercauteren
 Ivan Visconti
 Michael Walter
 Xiao Wang
 Udi Weinsberg
 Sophia Yabukov
 Yupeng Zhang
 Joe Zimmerman

Sponsoring Institutions



Dipartimento di Informatica, Università di Salerno, Italy



InfoCert, Rome, Italy



Università di Salerno, Italy

Abstracts of Invited Talks

Foundations of Blockchain Protocols

Aggelos Kiayias

School of Informatics, University of Edinburgh, 10 Crichton St.,
Edinburgh EH8 6AB, UK
Aggelos.Kiayias@ed.ac.uk

Abstract. The bitcoin system is a remarkable solution. But to what problem? The rise of bitcoin and other cryptocurrencies puts forth a wealth of interesting questions in distributed systems and cryptography that relate to building decentralized systems. We initiate a formal investigation of this class of protocols and of their basic properties.

The core of the bitcoin protocol can be abstracted in a simple algorithmic form that has been termed the bitcoin backbone in [1]. This work also provided a synchronous model for the analysis of the protocol. This algorithmic abstraction and modeling enabled the expression of simple provable properties about the blockchain data structure maintained by the protocol called chain quality, common prefix and chain growth. In this model, the concept of a robust transaction ledger can also be defined and analyzed as captured by its two basic properties, persistence and liveness. Given the above we show how a robust transaction ledger can be reduced to a blockchain protocol that satisfies these simple properties, cf. [2]. Alternative proof strategies are possible and will be also examined.

Given our formal definition of the robust transaction ledger problem, one can ask next whether the bitcoin backbone is the optimal solution. One important aspect of efficiency is the overhead to confirm transactions in the presence of an adversary, cf. [3], which is intimately related to the liveness of the ledger. Alternative designs such as GHOST used in the Ethereum system, are possible and will be analyzed and compared within the model with respect to their security and efficiency characteristics.

Finally, the relation of a robust transaction ledger to the consensus problem will be also examined and we will consider a number of model extensions that include rational players and dynamically changing user sets.

References

1. Garay, J.A., Kiayias, A., Leonardos, N.: The Bitcoin backbone protocol: analysis and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 281–310. Springer, Berlin

2. Kiayias, A., Panagiotakos, G.: Speed-Security Tradeoffs in Blockchain Protocols. IACR Cryptology ePrint Archive 2015: 1019 (2015)
3. Kiayias, A., Panagiotakos, G.: On Trees, Chains and Fast Transactions in the Blockchain. IACR Cryptology ePrint Archive 2016: 545 (2016)

Cryptography and Game Theory

Rafael Pass

Cornell Tech, New York, USA
rafael@cs.cornell.edu

Abstract. Cryptographic notions of knowledge consider the knowledge obtained, or possessed, by *computationally-bounded* agents under *adversarial* conditions. In this talk, we will survey some recent cryptographically-inspired approaches for reasoning about agents in the context of game-theory and mechanism design (where agents typically are modelled as computationally *unbounded*).

Contents

Encryption

A Tag Based Encoding: An Efficient Encoding for Predicate Encryption in Prime Order Groups	3
<i>Jongkil Kim, Willy Susilo, Fuchun Guo, and Man Ho Au</i>	
Non-zero Inner Product Encryption with Short Ciphertexts and Private Keys.	23
<i>Jie Chen, Benoît Libert, and Somindu C. Ramanna</i>	
Attribute-Based Encryption for Range Attributes.	42
<i>Nuttapong Attrapadung, Goichiro Hanaoka, Kazuto Ogawa, Go Ohtake, Hajime Watanabe, and Shota Yamada</i>	
Naor-Yung Paradigm with Shared Randomness and Applications	62
<i>Silvio Biagioni, Daniel Masny, and Daniele Venturi</i>	

Memory Protection

Provably-Secure Remote Memory Attestation for Heap Overflow Protection	83
<i>Alexandra Boldyreva, Taesoo Kim, Richard Lipton, and Bogdan Warinschi</i>	
Memory Erasability Amplification.	104
<i>Jan Camenisch, Robert R. Enderlein, and Ueli Maurer</i>	

Multi-party Computation

On Adaptively Secure Multiparty Computation with a Short CRS.	129
<i>Ran Cohen and Chris Peikert</i>	
Linear Overhead Optimally-Resilient Robust MPC Using Preprocessing.	147
<i>Ashish Choudhury, Emmanuela Orsini, Arpita Patra, and Nigel P. Smart</i>	
High-Precision Secure Computation of Satellite Collision Probabilities.	169
<i>Brett Hemenway, Steve Lu, Rafail Ostrovsky, and William Welser IV</i>	

Zero-Knowledge Proofs

Zero-Knowledge Made Easy so It Won't Make You Dizzy (A Tale of Transaction Put in Verse About an Illicit Kind of Commerce) 191
Trotta Gnam

Fiat–Shamir for Highly Sound Protocols Is Instantiable 198
Arno Mittelbach and Daniele Venturi

Verifiable Zero-Knowledge Order Queries and Updates for Fully Dynamic Lists and Trees 216
Esha Ghosh, Michael T. Goodrich, Olga Ohrimenko, and Roberto Tamassia

On the Implausibility of Constant-Round Public-Coin Zero-Knowledge Proofs 237
Yi Deng, Juan Garay, San Ling, Huaxiong Wang, and Moti Yung

Efficient Protocols

Improving Practical UC-Secure Commitments Based on the DDH Assumption 257
Eiichiro Fujisaki

The Whole is Less Than the Sum of Its Parts: Constructing More Efficient Lattice-Based AKEs 273
Rafael del Pino, Vadim Lyubashevsky, and David Pointcheval

Efficient Asynchronous Accumulators for Distributed PKI 292
Leonid Reyzin and Sophia Yakoubov

Outsourcing Computation

The Feasibility of Outsourced Database Search in the Plain Model 313
Carmit Hazay and Hila Zarosim

Verifiable Pattern Matching on Outsourced Texts 333
Dario Catalano, Mario Di Raimondo, and Simone Faro

Digital Signatures

Virtual Smart Cards: How to Sign with a Password and a Server 353
Jan Camenisch, Anja Lehmann, Gregory Neven, and Kai Samelin

Signatures Resilient to Uninvertible Leakage 372
Yuyu Wang, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka

Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions 391
Georg Fuchsbauer, Christian Hanser, Chethan Kamath, and Daniel Slamanig

Cryptanalysis

How (Not) to Instantiate Ring-LWE 411
Chris Peikert

Pen and Paper Arguments for SIMON and SIMON-like Designs 431
Christof Beierle

Two-party Computation

Bounded Size-Hiding Private Set Intersection 449
Tatiana Bradley, Sky Faber, and Gene Tsudik

On Garbling Schemes with and Without Privacy 468
Carsten Baum

What Security Can We Achieve Within 4 Rounds? 486
Carmit Hazay and Muthuramakrishnan Venkatasubramanian

Secret Sharing

Secret Sharing Schemes for Dense Forbidden Graphs 509
Amos Beimel, Oriol Farràs, and Naty Peter

Proactive Secret Sharing with a Dishonest Majority 529
Shlomi Dolev, Karim ElDefrawy, Joshua Lampkins, Rafail Ostrovsky, and Moti Yung

Obfuscation

Shorter Circuit Obfuscation in Challenging Security Models 551
Zvika Brakerski and Or Dagmi

Bounded KDM Security from iO and OWF 571
Antonio Marcedone, Rafael Pass, and Abhi Shelat

A Unified Approach to Idealized Model Separations via Indistinguishability Obfuscation 587
Matthew D. Green, Jonathan Katz, Alex J. Malozemoff, and Hong-Sheng Zhou

Author Index 605