# Lecture Notes in Computer Science 9841

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer

*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



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

---

A. Kiayias—Most of the work reported performed while at the National and Kapodistrian University of Athens. Research was supported by ERC project CODAMODA # 259152.

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*).

R. Pass—Supported in part by NSF Award CNS-1217821, NSF Award TWC-1561209, AFOSR Award FA9550-15-1-0262, a Microsoft Faculty Fellowship, and a Google Faculty Research Award.

# Contents

**Zero-Knowledge Proofs**



**Efficient Protocols**



**Outsourcing Computation**



**Digital Signatures**