

*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, Chennai, 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>

Dario Catalano · Roberto De Prisco (Eds.)

# Security and Cryptography for Networks

11th International Conference, SCN 2018  
Amalfi, Italy, September 5–7, 2018  
Proceedings

*Editors*

Dario Catalano  
University of Catania  
Catania  
Italy

Roberto De Prisco  
University of Salerno  
Fisciano  
Italy

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-98112-3              ISBN 978-3-319-98113-0 (eBook)  
<https://doi.org/10.1007/978-3-319-98113-0>

Library of Congress Control Number: 2018950389

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2018

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.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

The 11th Conference on Security and Cryptography for Networks (SCN 2018) was held in Amalfi, Italy, during September 5–7, 2018. The conference has traditionally been held in Amalfi, with the exception of the fifth edition, held in the nearby Maiori. After the editions of 1996, 1999 and 2002, it has been organized biannually thereafter.

In the digital era, communications crucially rely on computer networks. These allow both easy and fast access to information. At the same time, guaranteeing the security of modern communications is a delicate and challenging task. The SCN conference is an international meeting whose focus is on the cryptographic and information security methodologies needed to address such challenges. SCN allows researchers, practitioners, developers, and users interested in the security of communication networks to meet and exchange ideas in the wonderful scenario of the Amalfi Coast.

These proceedings contain the 30 papers that were selected by the Program Committee (PC). The conference received 66 submissions. Each submission was assigned to at least three reviewers, while submissions co-authored by PC members received, at least, four reviews. After an initial individual review phase, the submissions were discussed for a period of three additional weeks. During the discussion phase the PC used rather intensively a, recently introduced, feature of the review system, which allows PC members to anonymously ask questions directly to authors. The reviewing and selection procedure was a challenging and difficult task. We are deeply grateful to the PC members and external reviewers for the hard and careful work they did. Special thanks to Tancrede Lepoint, Giuseppe Persiano, and Antigoni Polychroniadou for their extra work as shepherds. Many thanks also to Michel Abdalla for his constant availability and for sharing with us his experience as former SCN Program Chair.

The conference program also included invited talks by Huijia Lin (University of California Santa Barbara, USA) and Eike Kiltz (Ruhr-University Bochum, Germany). We would like to thank both of them as well as all the other speakers for their contribution to the conference.

SCN 2018 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 setting up the system for us and for his assistance 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.

September 2018

Dario Catalano  
Roberto De Prisco

# SCN 2018

## The 11th Conference on Security and Cryptography for Networks

Amalfi, Italy  
September 5–7, 2018

### Program Chair

Dario Catalano                      Università di Catania, Italy

### 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

Elena Andreeva                KU Leuven, Belgium  
Manuel Barbosa                INESC TEC and FC Univers. do Porto, Portugal  
Carlo Blundo                    Università di Salerno, Italy  
Jean-Sébastien Coron        University of Luxembourg  
Mario Di Raimondo            Università di Catania, Italy  
Léo Ducas                      CWI, Amsterdam, The Netherlands  
Marc Fischlin                  Darmstadt University of Technology, Germany  
Pierre-Alain Fouque        University of Rennes, France

Georg Fuchsbauer	Inria and ENS, Paris, France
Romain Gay	ENS Paris, France
Carmit Hazay	Bar-Ilan University, Israel
Tancrède Lepoint	SRI International, USA
Gaëtan Leurent	Inria, France
Benoît Libert	CNRS and ENS de Lyon, France
Daniel Masny	UC Berkeley, USA
Svetla Nikova	KU Leuven, Belgium
Ryo Nishimaki	NTT, Japan
Luca Nizzardo	IMDEA Software Institute, Madrid, Spain
Emmanuela Orsini	University of Bristol, UK
Giuseppe Persiano	Università di Salerno, Italy
Thomas Peyrin	Nanyang Technological University, Singapore
Krzysztof Pietrzak	IST, Austria
Antigoni Polychroniadou	Cornell University, USA
Dominique Schröder	Friedrich-Alexander-Universität, Erlangen, Germany
Alessandra Scafuro	North Carolina State University, USA
Martijn Stam	University of Bristol, UK
Damien Stehlé	ENS de Lyon, France
Mehdi Tibouchi	NTT, Japan
Daniele Venturi	Università di Roma, La Sapienza, Italy
Damien Vergnaud	Sorbonne University and Institut Universitaire de France, Paris, France
Vanessa Vitse	Institut Fourier, University of Grenoble Alpes, France
Bogdan Warinschi	University of Bristol, UK

## Additional Reviewers

Aysajan Abidin	Thomas Espitau
Hamza Abusalah	Antonio Faonio
José Bacelar Almeida	David Galindo-Chacón
Miguel Ambrona	Ran Gelles
Nuttapong Attrapadung	Irene Giacomelli
Balthazar Bauer	Junqing Gong
Carsten Baum	Alonso Gonzalez
Pauline Bert	Antoine Joux
Carl Bootland	Karen Klein
Olivier Bronchain	Ilan Komargodski
Jie Chen	Russell W. F. Lai
Ilaria Chillotti	Kwangsue Lee
Michele Ciampi	Eleftheria Makri
Aisling Connolly	Giulio Malavolta
Jan Czakajowski	Chanathip Namprempre
Nico Doettling	Maria Naya-Plasencia

Khoa Nguyen  
Ariel Nof  
Cristina Onete  
Alain Passelègue  
Alice Pellet–Mary  
Olivier Pereira  
Rafael Del Pino  
Bernardo Portela  
Chen Qian  
Razvan Rosie  
Edouard Dufour Sans  
John Schank

Thomas Shrimpton  
Luisa Siniscalchi  
Christoph Striecks  
Junichi Tomida  
Ni Trieu  
Ida Tucker  
Furkan Turan  
Yohei Watanabe  
Tim Wood  
Takashi Yamakawa  
Avishay Yanai  
Ren Zhang

## IACR

This event was organized in cooperation with the International Association for Cryptologic Research (IACR).

## Sponsors



GRUPPO TECNOINVESTIMENTI

InfoCert, GRUPPO TECNOINVESTIMENTI, Rome, Italy



# Contents

## Signatures and Watermarking

Lower Bounds on Structure-Preserving Signatures for Bilateral Messages . . . . .	3
<i>Masayuki Abe, Miguel Ambrona, Miyako Ohkubo, and Mehdi Tibouchi</i>	
Fully Anonymous Group Signature with Verifier-Local Revocation . . . . .	23
<i>Ai Ishida, Yusuke Sakai, Keita Emura, Goichiro Hanaoka, and Keisuke Tanaka</i>	
Matrioska: A Compiler for Multi-key Homomorphic Signatures . . . . .	43
<i>Dario Fiore and Elena Pagnin</i>	
Unforgeable Watermarking Schemes with Public Extraction . . . . .	63
<i>Rupeng Yang, Man Ho Au, Junzuo Lai, Qiuliang Xu, and Zuoxia Yu</i>	

## Composability

Security Definitions for Hash Functions: Combining UCE and Indifferentiability . . . . .	83
<i>Daniel Jost and Ueli Maurer</i>	
A Constructive Perspective on Signcryption Security . . . . .	102
<i>Christian Badertscher, Fabio Banfi, and Ueli Maurer</i>	

## Encryption I

Tight Adaptively Secure Broadcast Encryption with Short Ciphertexts and Keys . . . . .	123
<i>Romain Gay, Lucas Kowalczyk, and Hoeteck Wee</i>	
Simulation-Based Receiver Selective Opening CCA Secure PKE from Standard Computational Assumptions . . . . .	140
<i>Keisuke Hara, Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka</i>	
Lizard: Cut Off the Tail! A Practical Post-quantum Public-Key Encryption from LWE and LWR . . . . .	160
<i>Jung Hee Cheon, Duhyeon Kim, Joohee Lee, and Yongsoo Song</i>	

## Multiparty Computation

Reducing Communication Channels in MPC . . . . .	181
<i>Marcel Keller, Dragos Rotaru, Nigel P. Smart, and Tim Wood</i>	
Proactive Secure Multiparty Computation with a Dishonest Majority . . . . .	200
<i>Karim Eldefrawy, Rafail Ostrovsky, Sunoo Park, and Moti Yung</i>	
From Fairness to Full Security in Multiparty Computation . . . . .	216
<i>Ran Cohen, Iftach Haitner, Eran Omri, and Lior Rotem</i>	
Efficient Scalable Multiparty Private Set-Intersection via Garbled Bloom Filters . . . . .	235
<i>Roi Inbar, Eran Omri, and Benny Pinkas</i>	

## Anonymity and Zero Knowledge

Semantically Secure Anonymity: Foundations of Re-encryption . . . . .	255
<i>Adam L. Young and Moti Yung</i>	
Securing Abe’s Mix-Net Against Malicious Verifiers via Witness Indistinguishability. . . . .	274
<i>Elette Boyle, Saleet Klein, Alon Rosen, and Gil Segev</i>	
Zero-Knowledge Protocols for Search Problems . . . . .	292
<i>Ben Berger and Zvika Brakerski</i>	

## Secret Sharing and Oblivious Transfer

Evolving Ramp Secret-Sharing Schemes . . . . .	313
<i>Amos Beimel and Hussien Othman</i>	
Actively Secure OT-Extension from $q$ -ary Linear Codes . . . . .	333
<i>Ignacio Cascudo, René Bødker Christensen, and Jaron Skovsted Gundersen</i>	

## Lattices and Post Quantum Cryptography

Estimate All the {LWE, NTRU} Schemes! . . . . .	351
<i>Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas Wunderer</i>	
More Efficient Commitments from Structured Lattice Assumptions . . . . .	368
<i>Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert</i>	

Quantum Demirci-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions . . . . .	386
<i>Akinori Hosoyamada and Yu Sasaki</i>	

## Obfuscation

Obfuscation from Polynomial Hardness: Beyond Decomposable Obfuscation . . . . .	407
<i>Yuan Kang, Chengyu Lin, Tal Malkin, and Mariana Raykova</i>	
Non-trivial Witness Encryption and Null-iO from Standard Assumptions . . . .	425
<i>Zvika Brakerski, Aayush Jain, Ilan Komargodski, Alain Passelègue, and Daniel Wichs</i>	

## Two-Party Computation

Secure Two-Party Computation over Unreliable Channels . . . . .	445
<i>Ran Gelles, Anat Paskin-Cherniavsky, and Vassilis Zikas</i>	
Combining Private Set-Intersection with Secure Two-Party Computation . . . .	464
<i>Michele Ciampi and Claudio Orlandi</i>	

## Protocols

Round-Reduced Modular Construction of Asymmetric Password-Authenticated Key Exchange . . . . .	485
<i>Jung Yeon Hwang, Stanislaw Jarecki, Taekyoung Kwon, Joohee Lee, Ji Sun Shin, and Jiayu Xu</i>	
On the Security Properties of e-Voting Bulletin Boards . . . . .	505
<i>Aggelos Kiayias, Annabell Kuldmaa, Helger Lipmaa, Janno Siim, and Thomas Zacharias</i>	

## Encryption II

Function-Revealing Encryption: Definitions and Constructions . . . . .	527
<i>Marc Joye and Alain Passelègue</i>	
Function-Hiding Inner Product Encryption Is Practical . . . . .	544
<i>Sam Kim, Kevin Lewi, Avradip Mandal, Hart Montgomery, Arnab Roy, and David J. Wu</i>	
Compact IBBE and Fuzzy IBE from Simple Assumptions . . . . .	563
<i>Junqing Gong, Benoît Libert, and Somindu C. Ramanna</i>	

<b>Author Index</b> . . . . .	583
-------------------------------	-----