Lecture Notes in Computer Science 6280

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

Juan A. Garay   Roberto De Prisco (Eds.)

Security and Cryptography for Networks

7th International Conference, SCN 2010
Amalfi, Italy, September 13-15, 2010
Proceedings

Springer

Volume Editors

Juan A. Garay
AT&T Labs Research
Florham Park, NJ 07932, USA
E-mail: garay@research.att.com

Roberto De Prisco
Università di Salerno, Dipartimento di Informatica ed Applicazioni
via Ponte don Melillo, 84084 Fisciano (SA), Italy
E-mail: robdep@dia.unisa.it

Library of Congress Control Number: 2010932603

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, J.1, G.2.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-15316-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-15316-7 Springer Berlin Heidelberg New York

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

The 7th Conference on Security and Cryptography for Networks (SCN 2010) was held in Amalfi, Italy, during September 13-15, 2010. This biennial conference has traditionally been held in Amalfi, with the exception of the fifth edition which was held in nearby Maiori. This year the conference received the financial support of the Department of "Informatica ed Applicazioni" and of the Faculty of Science of the University of Salerno, Italy.

The wide availability of computer networks, and in particular of the global Internet, offers the opportunity to perform electronically and in a distributed way a wide range of transactions. Hence, cryptography and security assume an increasingly important role in computer networks, both as critical enablers of new functionalities as well as warrantors of the mechanisms' soundness and safety. The principal aim of SCN as a conference is to bring together researchers in the above fields, with the goal of fostering cooperation and exchange of ideas in the stunning Amalfi Coast setting.

The conference received 94 submissions—a record-high number for the SCN conference series—in a broad range of cryptography and security areas, out of which 27 were accepted for publication in these proceedings on the basis of quality, originality, and relevance to the conference's scope. At least three Program Committee (PC) members—out of 27 world-renowned experts in the conference's various areas of interest—reviewed each submitted paper, while submissions co-authored by a PC member were subjected to the more stringent evaluation of five 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—almost as long as the initial individual reviewing period. The paper submission, review and discussion processes were effectively and efficiently made possible by the Web-Submission-and-Review software, written by Shai Halevi, and hosted by the International Association for Cryptologic Research (IACR). Many thanks to Shai for his assistance with the system's various features and constant availability.

Given the perceived quality of the submissions, the PC decided this year to give a Best Paper Award, both to celebrate the science and as a general way to promote outstanding work in the fields of cryptography and security and keep encouraging high-quality submissions to SCN. "Time-Specific Encryption," by Kenneth Paterson and Elizabeth Quaglia, was conferred such distinction.

Recent years have witnessed a rapid and prolific development of lattice- and "learning with errors" (LWE)-based cryptographic constructions, given the hardness and versatility of the underlying problems. The program was further enriched by the invited talk "Heuristics and Rigor in Lattice-Based Cryptography" by Chris Peikert (Georgia Institute of Technology), a world authority on the subject.

We finally 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 a truly intellectually stimulating one through their active participation.

September 2010

Juan A. Garay
Roberto De Prisco

SCN 2010

The 7th Conference on Security and Cryptography for Networks

September 13-15, 2010, Amalfi, Italy

Program Chair

Juan A. Garay	AT&T Labs – Research, USA

General Chair

Roberto De Prisco	Università di Salerno, Italy

Program Committee

Xavier Boyen	University of Liege, Belgium
Christian Cachin	IBM Research, Switzerland
Haowen Chan	Carnegie Mellon University, USA
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Yevgeniy Dodis	New York University, USA
Marc Fischlin	Darmstadt University of Technology, Germany
Rosario Gennaro	IBM Research, USA
Martin Hirt	ETH Zürich, Switzerland
Dennis Hofheinz	Karlsruhe Institute of Technology, Germany
Ari Juels	RSA Laboratories, USA
Kaoru Kurosawa	Ibaraki University, Japan
Tal Malkin	Columbia University, USA
John Mitchel	Stanford University, USA
David Naccache	ENS Paris, France
Antonio Nicolosi	Stevens Institute of Technology, USA
Jesper Nielsen	University of Aarhus, Denmark
Kobbi Nissim	Microsoft ILDC and Ben-Gurion University, Israel
Krzysztof Pietrzak	CWI, The Netherlands
Christian Rechberger	K.U. Leuven, Belgium
Vincent Rijmen	K.U. Leuven, Belgium and TU Graz, Austria
Guy Rothblum	Princeton University/IAS, USA
Berry Schoenmakers	TU Eindhoven, The Netherlands
Martijn Stam	EPFL, Switzerland
Vinod Vaikuntanathan	IBM Research, USA

Ivan Visconti	Università di Salerno, Italy
Shabsi Walfish	Google Inc., USA
Hoeteck Wee	Queens College, CUNY, USA

Organizing Committee

Aniello Castiglione	Università di Salerno, Italy
Paolo D'Arco	Università di Salerno, Italy

Steering Committee

Carlo Blundo	Università di Salerno, Italy
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 Paris, France
Douglas Stinson	University of Waterloo, Canada
Gene Tsudik	University of California - Irvine, USA
Moti Yung	Google Inc. and Columbia University, USA

External Reviewers

Divesh Aggarwal
Laila El Aimani
Kfir Barhum
Rikke Bendlin
Allison Bishop
Carl Bosley
Kevin Bowers
Christophe De Cannière
Ashish Choudary
Seung Geol Choi
Sherman Chow
Dana Dachman-Soled
Özgür Dagdelen
Pooya Farshim
Nelly Fazio
Matthias Fitzi
David Freeman
Eiichiro Fujisaki
Robert Granger
Matthew Green
Jens Groth
Mike Hamburg
Kris Haralambiev
Carmit Hazay
Javier Herranz
Sebastiaan Indesteege
Yuval Ishai
Charanjit Jutla
Alexandre Karlov
Jonathan Katz
Shahram Khazaei
Dmitry Khovratovich
Kazukuni Kobara
Chiu Yuen Koo
Anja Lehmann
Benoit Libert
Adriana Lopez-Alt
Christoph Lucas
Philip Mackenzie
Mark Manulis
Breno de Medeiros
Phong Nguyen
Adam O'Neil
Cristina Onete
Claudio Orlandi
Onur Özen
C. Pandu Rangan
Le Trieu Phong
Bartosz Przydatek
Juraj Šarinay
Alessandra Scafuro
Joern-Marc Schmidt
Michael Schneider
Dominique Schröder
Marc Stevens
Björn Tackmann
Aris Tentes
Stefano Tessaro
Tomas Toft
Yevgeniy Vahlis
Vincent Verneuil
Enav Weinreb
Daniel Wichs
Vassilis Zikas

Table of Contents

Encryption I

Invited Talk

Cryptanalysis

Hash Functions

Side Channel Attacks and Leakage Resilience

Encryption II

Cryptographic Protocols I

Authentication and Key Agreement

Cryptographic Primitives and Schemes

Lattice-Based Cryptography

Groups Signatures and Authentication

Cryptographic Protocols II

Anonymity