Lecture Notes in Computer Science 8642

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

Michel Abdalla Roberto De Prisco (Eds.)

Security and Cryptography for Networks

9th International Conference, SCN 2014
Amalfi, Italy, September 3-5, 2014
Proceedings

Springer

Volume Editors

Michel Abdalla
École Normale Supérieure & CNRS
45 rue d'Ulm
75005 Paris, France
E-mail: michel.abdalla@ens.fr

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-10878-0 e-ISBN 978-3-319-10879-7
DOI 10.1007/978-3-319-10879-7
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014946896

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 9th Conference on Security and Cryptography for Networks (SCN 2014) was held in Amalfi, Italy, during September 3-5, 2014. The conference has traditionally been held in Amalfi, with the exception of the fifth edition which 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 information infrastructures rely heavily on computer networks with the Internet being the one that is most used. Implementing secure distributed transactions for such networks poses new challenges. The SCN conference is an international meeting that focuses on cryptographic and information security tools, both from a theoretical and from a practical perspective, that are needed to face the above challenges. SCN gives to researchers, practitioners, developers, and users interested in the security of communication networks, the possibility to foster cooperation and to exchange techniques, tools, experiences, and ideas in the stunning Amalfi Coast setting.

The conference received 95 submissions in a broad range of cryptography and security areas, setting a new record number of submissions for SCN. The selection of the papers was a difficult task. Amongst the many high-quality submissions, 31 were accepted for publication in these proceedings on the basis of quality, originality, and relevance to the conference's scope.

The international Program Committee (PC) consisted of 33 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 Brett Hemenway, Giuseppe Persiano, and Ivan Visconti, for their extra work as shepherds.

Given the perceived quality of the submissions, the PC also decided to give a best paper award, both to promote outstanding work in the fields of cryptography and information security and to keep encouraging high-quality submissions to SCN. This award was given to the paper "On the Classification of Finite Boolean Functions up to Fairness" by Nikolaos Makriyannis.

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 at École Normale Supérieure. Many thanks to Shai for his assistance with the system's various features and constant availability.

The program was further enriched by the invited talks of Dario Catalano (University of Catania, Italy) Sanjam Garg (IBM T.J. Watson Research Center,

USA), and Hoeteck Wee (École Normale Supérieure, France), top experts on the subjects of the conference.

SCN 2014 was organized in cooperation with the International Association for Cryptologic Research (IACR).

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 a truly intellectually stimulating one through their active participation.

We finally thank the *Dipartimento di Informatica* of the University of Salerno, Italy, for the financial support.

September 2014

Michel Abdalla
Roberto De Prisco

SCN 2014

The 9th Conference on
Security and Cryptography for Networks

Amalfi, Italy
September 3–5, 2014

Organized by

Dipartimento di Informatica
Università di Salerno

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

Program Chair

Michel Abdalla	ENS and CNRS, France

General Chair

Roberto De Prisco	Università di Salerno, Italy

Organizing Committee

Aniello Castiglione	Università di Salerno, Italy
Luigi Catuogno	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, France
Douglas Stinson	University of Waterloo, Canada
Gene Tsudik	University of California - Irvine, USA
Moti Yung	Google, USA and Columbia University, USA

Program Committee

Masayuki Abe	NTT, Japan
Giuseppe Ateniese	Rome University, Italy
Nuttapong Attrapadung	AIST, Japan
Olivier Blazy	Ruhr-Universität Bochum, Germany
Carlo Blundo	Università di Salerno, Italy
Elette Boyle	Technion, Israel
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Stefan Dziembowski	University of Warsaw, Poland
Dario Fiore	IMDEA, Spain
Marc Fischlin	Darmstadt University of Technology, Germany
Pierre-Alain Fouque	University of Rennes, France
Brett Hemenway	University of Pennsylvania, USA
Stanislaw Jarecki	University of California - Irvine, USA
Gaëtan Leurent	Inria, France
Daniele Micciancio	University of California - San Diego, USA
Michael Naehrig	Microsoft Research, USA
Adam O'Neill	Georgetown University, USA
Claudio Orlandi	Aarhus University, Denmark
Carles Padró	Nanyang Technological University, Singapore
Christopher Peikert	Georgia Institute of Technology, USA
Giuseppe Persiano	Università di Salerno, Italy
Thomas Peyrin	Nanyang Technological University, Singapore
Emmanuel Prouff	ANSSI, France
Christian Rechberger	DTU, Denmark
Vincent Rijmen	K.U. Leuven, Belgium
Christian Schaffner	University of Amsterdam, The Netherlands
Thomas Shrimpton	Portland State University, USA
François-Xavier Standaert	Université catholique de Louvain, Belgium
Stefano Tessaro	University of California - Santa Barbara, USA
Mehdi Tibouchi	NTT, Japan
Damien Vergnaud	ENS, France
Ivan Visconti	University of Salerno, Italy
Bogdan Warinschi	University of Bristol, UK

External Reviewers

Mohamed Abdelraheem	Ilario Bonacina	Dario Catalano
Hoda A. Alkhzaimi	Joppe W. Bos	Nishanth Chandran
Jacob Alperin-Sheriff	Niek Bouman	Melissa Chase
Marcin Andrychowicz	Hank Carter	Jie Chen
Gilad Asharov	Henry Carter	Céline Chevalier
Abhishek Banerjee	Ignacio Cascudo	Craig Costello
Céline Blondeau	David Cash	Dana Dachman-Soled

Bernardo David
Léo Ducas
Keita Emura
Anna Lisa Ferrara
Nils Fleischhacker
Jean-Pierre Flori
Georg Fuchsbauer
Benjamin Fuller
Irene Giacomelli
Vincent Grosso
Dennis Hofheinz
Vincenzo Iovino
Ioana Ivan
Amandine Jambert
Abhishek Jain
Jérémy Jean
Hugo Jonker
Saqib A. Kakvi
Eike Kiltz
Taechan Kim
Susumu Kiyoshima
François Koeune
Hugo Krawczyk
Wang Lei
Patrick Longa
Vadim Lyubashevsky
Daniel Malinowski
Takahiro Matsuda
Sarah Meiklejohn
Diego Mirandola
Ivica Nikolic
Ryo Nishimaki
Miyako Ohkubo
Jiaxin Pan
Maura Paterson
Thomas Peters
Ananth Raghunathan
Samuel Ranellucci
Thomas Roche
Yusuke Sakai
Benedikt Schmidt
Dominique Schroder
Maciej Skórski
Gabriele Spini
Mario Strefler
Katsuyuki Takashima
Tyge Tiessen
Gaven Watson
Hoeteck Wee
Shota Yamada
Eugen Zalinescu
Bingsheng Zhang

Abstracts of Invited Talks

Program Obfuscation via Multilinear Maps

Sanjam Garg

IBM T.J. Watson
sanjamg@cs.ucla.edu

Abstract. Recent proposals for plausible candidate constructions of *multilinear maps* and *obfuscation* have radically transformed what we imagined to be possible in cryptography. For over a decade cryptographers had been very skeptical about the existence of such objects. In this article, we provide a very brief introduction to these results and some of their interesting consequences.

Functional Encryption and Its Impact on Cryptography

Hoeteck Wee*

ENS, Paris, France
wee@di.ens.fr

Abstract. Functional encryption is a novel paradigm for public-key encryption that enables both fine-grained access control and selective computation on encrypted data, as is necessary to protect big, complex data in the cloud. In this article, we provide a brief introduction to functional encryption, and an overview of its overarching impact on the field of cryptography.

* CNRS (UMR 8548) and INRIA. Supported in part by NSF Awards CNS-1237429 and CNS-1319021 and a fellowship from the Alexander von Humboldt Foundation.

Homomorphic Signatures and Message Authentication Codes

Dario Catalano

Università di Catania, Italy
catalano@dmi.unict.it

Abstract. Homomorphic message authenticators allow to validate computation on previously signed data. The holder of a dataset $\{m_1, \ldots, m_\ell\}$ uses her secret key sk to produce corresponding tags $(\sigma_1, \ldots, \sigma_\ell)$ and stores the authenticated dataset on a remote server. Later the server can (publicly) compute $m = f(m_1, \ldots, m_\ell)$ together with a succinct tag σ certifying that m is the correct output of the computation f. A nice feature of homomorphic authenticators is that the validity of this tag can be verified *without* having to know the original dataset. This latter property makes the primitive attractive in a variety of context and applications, including, for instance, verifiable delegation of computation on outsourced data.

In this short survey, I will give an overview of the state of the art in the areas of homomorphic signatures and message authentication codes. I will (briefly) describe some of the most recent results and provide an overview of the main challenges that remain to address.

Table of Contents

Network Security

Functional Encryption

Invited Talk II

Cryptanalysis

Secure Computation – Implementation

Zero Knowledge

Message Authentication

Invited Talk III

Proofs of Space and Erasure

Public-Key Encryption