

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, 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, Saarbruecken, Germany

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

© Springer International Publishing Switzerland 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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 Streffer
Katsuyuki Takashima
Tyge Tiessen
Gaven Watson
Hoeteck Wee
Shota Yamada
Eugen Zalescu
Bingsheng Zhang

Abstracts of Invited Talks

Program Obfuscation via Multilinear Maps

Sanjam Garg

IBM T.J. Watson

`sanjam@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@dmf.unict.it`

Abstract. Homomorphic message authenticators allow to validate computation on previously signed data. The holder of a dataset $\{m_1, \dots, m_\ell\}$ uses her secret key \mathbf{sk} to produce corresponding tags $(\sigma_1, \dots, \sigma_\ell)$ and stores the authenticated dataset on a remote server. Later the server can (publicly) compute $m = f(m_1, \dots, m_\ell)$ 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

Key Exchange

Universally Composable Non-Interactive Key Exchange	1
<i>Eduarda S.V. Freire, Julia Hesse, and Dennis Hofheinz</i>	
Forward Secure Non-Interactive Key Exchange	21
<i>David Pointcheval and Olivier Sanders</i>	
Secure Key Exchange and Sessions without Credentials	40
<i>Ran Canetti, Vladimir Kolesnikov, Charles Rackoff, and Yevgeniy Vahlis</i>	

Multilinear Maps and Obfuscation

Relaxed Two-to-One Recoding Schemes	57
<i>Omkant Pandey, Kim Ramchen, and Brent Waters</i>	
Obfuscation \Rightarrow (IND-CPA Security \nRightarrow Circular Security)	77
<i>Antonio Marcedone and Claudio Orlandi</i>	

Invited Talk I

Program Obfuscation via Multilinear Maps	91
<i>Sanjam Garg</i>	

Pseudorandom Function Extensions

Constrained Verifiable Random Functions	95
<i>Georg Fuchsbaauer</i>	
Publicly Evaluable Pseudorandom Functions and Their Applications . . .	115
<i>Yu Chen and Zongyang Zhang</i>	

Secure Computation – Foundations and Algorithms

On the Classification of Finite Boolean Functions up to Fairness	135
<i>Nikolaos Makriyannis</i>	
Communication-Efficient MPC for General Adversary Structures	155
<i>Joshua Lampkins and Rafail Ostrovsky</i>	
Publicly Auditable Secure Multi-Party Computation	175
<i>Carsten Baum, Ivan Damgård, and Claudio Orlandi</i>	

Reducing the Overhead of MPC over a Large Population	197
<i>Ashish Choudhury, Arpita Patra, and Nigel P. Smart</i>	

Network Security

Statistics on Password Re-use and Adaptive Strength for Financial Accounts	218
<i>Daniel V. Bailey, Markus Dürmuth, and Christof Paar</i>	

Efficient Network-Based Enforcement of Data Access Rights	236
<i>Paul Giura, Vladimir Kolesnikov, Aris Tentes, and Yevgeniy Vahlis</i>	

EyeDecrypt — Private Interactions in Plain Sight	255
<i>Andrea G. Forte, Juan A. Garay, Trevor Jim, and Yevgeniy Vahlis</i>	

Functional Encryption

Semi-adaptive Attribute-Based Encryption and Improved Delegation for Boolean Formula	277
<i>Jie Chen and Hoeteck Wee</i>	

Expressive Attribute-Based Encryption with Constant-Size Ciphertexts from the Decisional Linear Assumption	298
<i>Katsuyuki Takashima</i>	

Invited Talk II

Functional Encryption and Its Impact on Cryptography	318
<i>Hoeteck Wee</i>	

Cryptanalysis

Generic Attacks on Strengthened HMAC: n -bit Secure HMAC Requires Key in All Blocks	324
<i>Yu Sasaki and Lei Wang</i>	

Improved Indifferentiable Security Analysis of PHOTON	340
<i>Yusuke Naito and Kazuo Ohta</i>	

Secure Computation – Implementation

Faster Maliciously Secure Two-Party Computation Using the GPU	358
<i>Tore Kasper Frederiksen, Thomas P. Jakobsen, and Jesper Buus Nielsen</i>	

Systematizing Secure Computation for Research and Decision Support	380
<i>Jason Perry, Debayan Gupta, Joan Feigenbaum, and Rebecca N. Wright</i>	

An Empirical Study and Some Improvements of the MiniMac Protocol for Secure Computation.....	398
<i>Ivan Damgård, Rasmus Lauritsen, and Tomas Toft</i>	

Zero Knowledge

Efficient NIZK Arguments via Parallel Verification of Benes Networks	416
<i>Helger Lipmaa</i>	

Non-Malleable Zero Knowledge: Black-Box Constructions and Definitional Relationships	435
<i>Abhishek Jain and Omkant Pandey</i>	

On Adaptively Secure Protocols	455
<i>Muthuramakrishnan Venkitasubramaniam</i>	

Message Authentication

Key-Indistinguishable Message Authentication Codes	476
<i>Joël Alwen, Martin Hirt, Ueli Maurer, Arpita Patra, and Pavel Raykov</i>	

Interactive Encryption and Message Authentication	494
<i>Yevgeniy Dodis and Dario Fiore</i>	

Invited Talk III

Homomorphic Signatures and Message Authentication Codes	514
<i>Dario Catalano</i>	

Proofs of Space and Erasure

Efficient Proofs of Secure Erasure	520
<i>Nikolaos P. Karvelas and Aggelos Kiayias</i>	

Proofs of Space: When Space Is of the Essence.....	538
<i>Giuseppe Ateniese, Ilario Bonacina, Antonio Faonio, and Nicola Galesi</i>	

Public-Key Encryption

Chosen Ciphertext Security on Hard Membership Decision Groups: The Case of Semi-smooth Subgroups of Quadratic Residues	558
<i>Takashi Yamakawa, Shota Yamada, Koji Nuida, Goichiro Hanaoka, and Noboru Kunihiro</i>	
On Selective-Opening Attacks against Encryption Schemes	578
<i>Rafail Ostrovsky, Vanishree Rao, and Ivan Visconti</i>	
Narrow Bandwidth Is Not Inherent in Reverse Public-Key Encryption	598
<i>David Naccache, Rainer Steinwandt, Adriana Suárez Corona, and Moti Yung</i>	
Author Index	609