

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

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

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

Ivan Visconti Roberto De Prisco (Eds.)

Security and Cryptography for Networks

8th International Conference, SCN 2012
Amalfi, Italy, September 5-7, 2012
Proceedings

Volume Editors

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

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-32927-2 e-ISBN 978-3-642-32928-9
DOI 10.1007/978-3-642-32928-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012945012

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2.0, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

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 8th Conference on Security and Cryptography for Networks (SCN 2012) was held in Amalfi, Italy, during September 5–7, 2012. This biennial conference has traditionally been held in Amalfi, with the exception of the fifth edition which was held in nearby Maiori.

The world-wide use of computer networks, and in particular of the Internet, opens new challenges for the security of electronic and distributed transactions. Cryptography and information security must face both the theoretical and practical aspects of the above challenges, by providing concepts, techniques, applications, and practical experiences. The principal aim of SCN as a conference is to bring together researchers, practitioners, developers, and users interested in the above fields, to foster cooperation and to exchange techniques, tools, experiences, and ideas in the stunning Amalfi Coast setting.

The conference received 72 submissions in a broad range of cryptography and security areas. The selection of papers was a difficult task. This year we received many high-quality submissions and 31 of them 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 28 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 for his constant availability.

Given the perceived quality of the submissions, the PC decided also this year 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. “Deterministic Public Key Encryption and Identity-Based Encryption from Lattices in the Auxiliary-Input Setting” by Xiang Xie, Rue Xue, and Rui Zhang was conferred such distinction.

The program was further enriched by the invited talks of Yuval Ishai (Technion, Israel) and Giuseppe Persiano (Università di Salerno, Italy), top experts on the subjects of the conference.

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 2012

Ivan Visconti
Roberto De Prisco

SCN 2012

The 8th Conference on Security and Cryptography for Networks

September 5–7, 2012, Amalfi, Italy

Program Chair

Ivan Visconti

Università di Salerno, Italy

Program Committee

Masayuki Abe

NTT, Japan

Amos Beimel

Ben-Gurion University, Israel

Carlo Blundo

Università di Salerno, Italy

Alexandra Boldyreva

Georgia Institute of Technology, USA

Xavier Boyen

PARC, USA

Dario Catalano

University of Catania, Italy

Melissa Chase

Microsoft Research Redmond, USA

Dana Dachman-Soled

Microsoft Research New England, USA

Stefan Dziembowski

University of Warsaw, Poland and Sapienza

University of Rome, Italy

Pierre-Alain Fouque

ENS, France

Juan Garay

AT&T Labs-Research, USA

Vipul Goyal

Microsoft Research, India

Brett Hemenway

University of Michigan, USA

Martin Hirt

ETH Zurich, Switzerland

Dennis Hofheinz

Karlsruhe Institute of Technology, Germany

Stanislaw Jarecki

UCI, USA

Gregory Neven

IBM Research, Switzerland

Carles Padro

Nanyang Technological University, Singapore

Benny Pinkas

Bar Ilan University, Israel, and Google, USA

Bart Preneel

Katholieke Universiteit Leuven, Belgium

Matt Robshaw

Orange Labs, France

Alon Rosen

IDC Herzliya, Israel

abhi shelat

University of Virginia, USA

Francois-Xavier Standaert

UCL, Belgium

Dominique Unruh

University of Tartu, Estonia

Bogdan Warinschi

University of Bristol, UK

Daniel Wichs

IBM T.J. Watson Research Center, USA

Moti Yung

Google, USA and Columbia University, USA

General Chair

Roberto De Prisco

Università di Salerno, Italy

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, USA and Columbia University, USA

External Reviewers

Shweta Agrawal

Clemente Galdi

Ilan Orlov

Giulia Alberini

Chaya Ganesh

Chris Peikert

Joël Alwen

Peter Gaži

Vanishree Rao

Gilad Asharov

Clint Givens

Mariana Raykova

Abhishek Banerjee

Dov Gordon

Elizabeth Quaglia

Steven Bellovin

Divya Gupta

Alessandra Scafuro

Charles Bouillaguet

Tibor Jager

Hakan Seyalioglu

David Cash

Jeremy Jean

Adam Smith

Iwen Coisel

Tomasz Kazana

Adam Stubblefield

Sandro Coretti

François Koeune

Björn Tackmann

Reza Curtmola

Stephan Krenn

Yevgeniy Vahlis

Gregory Demay

Huijia Lin

Jorge L. Villar

Patrick Derbez

Steve Lu

Keita Xagawa

Mario Di Raimondo

Christoph Lucas

Vassilis Zikas

Laila El Aïmani

Benjamin Martin

Yunlei Zhao

Oriol Farràs

Christian Matt

Hong-Sheng Zhou

Dario Fiore

Irippuge Milinda Perera

Atsushi Fujioka

Miyako Ohkubo

Table of Contents

Cryptography from Lattices

Deterministic Public Key Encryption and Identity-Based Encryption from Lattices in the Auxiliary-Input Setting	1
<i>Xiang Xie, Rui Xue, and Rui Zhang</i>	
Ring Switching in BGV-Style Homomorphic Encryption	19
<i>Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart</i>	
Zero-Knowledge Proofs with Low Amortized Communication from Lattice Assumptions	38
<i>Ivan Damgård and Adriana López-Alt</i>	
Fully Anonymous Attribute Tokens from Lattices	57
<i>Jan Camenisch, Gregory Neven, and Markus Rückert</i>	

Signature Schemes

Efficient Structure-Preserving Signature Scheme from Standard Assumptions	76
<i>Jan Camenisch, Maria Dubovitskaya, and Kristiyan Haralambiev</i>	
Compact Round-Optimal Partially-Blind Signatures	95
<i>Olivier Blazy, David Pointcheval, and Damien Vergnaud</i>	
History-Free Sequential Aggregate Signatures	113
<i>Marc Fischlin, Anja Lehmann, and Dominique Schröder</i>	
A New Hash-and-Sign Approach and Structure-Preserving Signatures from DLIN	131
<i>Melissa Chase and Markulf Kohlweiss</i>	

Encryption Schemes I

Blackbox Construction of a More Than Non-Malleable CCA1 Encryption Scheme from Plaintext Awareness	149
<i>Steven Myers, Mona Sergi, and abhi shelat</i>	
Decentralized Dynamic Broadcast Encryption	166
<i>Duong Hieu Phan, David Pointcheval, and Mario Strefler</i>	

Time-Specific Encryption from Forward-Secure Encryption	184
<i>Kohei Kasamatsu, Takahiro Matsuda, Keita Emura,</i> <i>Nuttapong Attrapadung, Goichiro Hanaoka, and</i> <i>Hideki Imai</i>	

Efficient Two-Party and Multi-Party Computation

Improved Secure Two-Party Computation via Information-Theoretic Garbled Circuits	205
<i>Vladimir Kolesnikov and Ranjit Kumaresan</i>	
5PM: Secure Pattern Matching	222
<i>Joshua Baron, Karim El Defrawy, Kirill Minkovich,</i> <i>Rafail Ostrovsky, and Eric Tressler</i>	
Implementing AES via an Actively/Covertly Secure Dishonest-Majority MPC Protocol	241
<i>Ivan Damgård, Marcel Keller, Enrique Larraia,</i> <i>Christian Miles, and Nigel P. Smart</i>	

Security in the UC Framework

On the Centrality of Off-Line E-Cash to Concrete Partial Information Games	264
<i>Seung Geol Choi, Dana Dachman-Soled, and Moti Yung</i>	
Universally Composable Security with Local Adversaries	281
<i>Ran Canetti and Margarita Vald</i>	

Cryptanalysis

On the Strength Comparison of the ECDLP and the IFP	302
<i>Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, and Tetsuya Izu</i>	
New Attacks for Knapsack Based Cryptosystems	326
<i>Gottfried Herold and Alexander Meurer</i>	
Multiple Differential Cryptanalysis Using LLR and χ^2 Statistics	343
<i>Céline Blondeau, Benoît Gérard, and Kaisa Nyberg</i>	
Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-commutative Rings	361
<i>Enrico Thomae</i>	

Encryption Schemes II

Homomorphic Encryption for Multiplications and Pairing Evaluation . . .	374
<i>Guilhem Castagnos and Fabien Laguillaumie</i>	
Publicly Verifiable Ciphertexts	393
<i>Juan Manuel González Nieto, Mark Manulis, Bertram Poettering, Jothi Rangasamy, and Douglas Stebila</i>	
Public-Key Encryption with Lazy Parties	411
<i>Kenji Yasunaga</i>	

Efficient Constructions

Probabilistically Correct Secure Arithmetic Computation for Modular Conversion, Zero Test, Comparison, MOD and Exponentiation	426
<i>Ching-Hua Yu and Bo-Yin Yang</i>	
MAC Aggregation with Message Multiplicity	445
<i>Vladimir Kolesnikov</i>	
Efficiency Limitations of Σ -Protocols for Group Homomorphisms Revisited	461
<i>Björn Terelius and Douglas Wikström</i>	
A More Efficient Computationally Sound Non-Interactive Zero-Knowledge Shuffle Argument	477
<i>Helger Lipmaa and Bingsheng Zhang</i>	

Protocols and Combiners

Active Security in Multiparty Computation over Black-Box Groups . . .	503
<i>Yvo Desmedt, Josef Pieprzyk, and Ron Steinfeld</i>	
Hash Combiners for Second Pre-image Resistance, Target Collision Resistance and Pre-image Resistance Have Long Output	522
<i>Arno Mittelbach</i>	
Human Perfectly Secure Message Transmission Protocols and Their Applications	540
<i>Stelios Erotokritou and Yvo Desmedt</i>	
Oblivious Transfer with Hidden Access Control from Attribute-Based Encryption	559
<i>Jan Camenisch, Maria Dubovitskaya, Robert R. Enderlein, and Gregory Neven</i>	

Author Index	581
------------------------	-----