

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Rafail Ostrovsky Roberto De Prisco
Ivan Visconti (Eds.)

Security and Cryptography for Networks

6th International Conference, SCN 2008
Amalfi, Italy, September 10-12, 2008
Proceedings

Volume Editors

Rafail Ostrovsky
University of California, Los Angeles
Department of Computer Science
Box 951596, 3732D BH, Los Angeles, CA, 90095-1596, USA
E-mail: rafail@cs.ucla.edu

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

Ivan Visconti
Università di Salerno
Dipartimento di Informatica ed Applicazioni
via Ponte don Melillo, 84084 Fisciano (SA), Italy
E-mail: visconti@dia.unisa.it

Library of Congress Control Number: 2008933864

CR Subject Classification (1998): E.3, C.2, D.4.6, K.4.1, K.4.4, K.6.5, F.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-85854-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-85854-6 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12512393 06/3180 5 4 3 2 1 0

Preface

The 6th Conference on Security and Cryptography for Networks (SCN 2008) was held in Amalfi, Italy, on September 10–12, 2008. The first four editions of the conference were held in Amalfi, while, two years ago, the fifth edition was held in the nearby Maiori. This year we moved back to the traditional location.

Security and privacy are increasing concerns in computer networks such as the Internet. The availability of fast, reliable, and cheap electronic communication offers the opportunity to perform, electronically and in a distributed way, a wide range of transactions of a most diverse nature. The conference brought together researchers in the fields of cryptography and security in communication networks with the goal of fostering cooperation and exchange of ideas. The main topics of the conference this year included anonymity, implementations, authentication, symmetric-key cryptography, complexity-based cryptography, privacy, cryptanalysis, cryptographic protocols, digital signatures, public-key cryptography, hash functions, identification.

The international Program Committee consisted of 24 members who are top experts in the conference fields. The PC received 71 submissions and selected 26 papers for presentation at the conference. These proceedings include the 26 accepted papers and the abstract of the invited talk by Shai Halevi.

The PC selected papers on the basis of originality, quality and relevance to the conference scope. Due to the high number of submissions, paper selection was a difficult task and many good papers had to be rejected. Each paper was refereed by three or four reviewers. We thank the members of the PC for the effort invested in the selection process. We also gratefully acknowledge the help of the external reviewers who evaluated submissions in their area of expertise. The names of these reviewers are listed on page VIII, and we apologize for any inadvertent omissions or mistakes.

Finally, we would like to thank the authors of all submitted papers and the conference participants, who ultimately made this conference possible.

September 2008

R. Ostrovsky
R. De Prisco
I. Visconti

Referees

Divesh Aggarwal	Alejandro Hevia	Christopher Portmann
Zuzana Beerliova	Dennis Hofheinz	Emmanuel Prouff
Charles Bouillaguet	Susan Hohenberger	Dominik Raub
Suresh Chari	Emeline Hufschmitt	Mike Rosulek
Debbie Cook	Charanjit Jutla	Amit Sahai
Cécile Delerablée	Bhavana Kanukurthi	Christian Schaffner
Mario Di Raimondo	Aggelos Kiayias	Nigel Smart
Orr Dunkelman	Eike Kiltz	Stefano Tessaro
Dario Fiore	Vladimir Kolesnikov	Carmine Ventre
Sebastian Gajek	Gaëtan Leurent	Enav Weinreb
David Galindo	Anna Lysyanskaya	Daniel Wichs
Peter Gaži	Vadim Lyubashevsky	Vassilis Zikas
Craig Gentry	Alexander May	Cliff Changchun Zou
Sharon Goldberg	Lorenz Minder	
Amir Herzberg	David Molnar	

Table of Contents

Invited Talk

Storage Encryption: A Cryptographer's View (Abstract)	1
<i>Shai Halevi</i>	

Session 1: Implementations

Implementing Two-Party Computation Efficiently with Security against Malicious Adversaries	2
<i>Yehuda Lindell, Benny Pinkas, and Nigel P. Smart</i>	
CLL: A Cryptographic Link Layer for Local Area Networks	21
<i>Yves Igor Jerschow, Christian Lochert, Björn Scheuermann, and Martin Mauve</i>	
Faster Multi-exponentiation through Caching: Accelerating (EC)DSA Signature Verification	39
<i>Bodo Möller and Andy Rupp</i>	

Session 2: Protocols I

Privacy Preserving Data Mining within Anonymous Credential Systems	57
<i>Aggelos Kiayias, Shouhuai Xu, and Moti Yung</i>	
Improved Privacy of the Tree-Based Hash Protocols Using Physically Unclonable Function	77
<i>Julien Bringer, Hervé Chabanne, and Thomas Icart</i>	

Session 3: Encryption I

Two Generic Constructions of Probabilistic Cryptosystems and Their Applications	92
<i>Guilhem Castagnos</i>	
Cramer-Shoup Satisfies a Stronger Plaintext Awareness under a Weaker Assumption	109
<i>Isamu Teranishi and Wakaha Ogata</i>	

Session 4: Encryption II

General Certificateless Encryption and Timed-Release Encryption	126
<i>Sherman S.M. Chow, Volker Roth, and Eleanor G. Rieffel</i>	

Efficient Certificate-Based Encryption in the Standard Model 144
Joseph K. Liu and Jianying Zhou

Session 5: Primitives

An Improved Robust Fuzzy Extractor 156
Bhavana Kanukurthi and Leonid Reyzin

On Linear Secret Sharing for Connectivity in Directed Graphs 172
Amos Beimel and Anat Paskin

Session 6: Signatures

Expressive Subgroup Signatures 185
Xavier Boyen and Cécile Delerablée

Anonymous Proxy Signatures 201
Georg Fuchsbauer and David Pointcheval

Multisignatures Using Proofs of Secret Key Possession, as Secure as the
 Diffie-Hellman Problem 218
Ali Bagherzandi and Stanisław Jarecki

Session 7: Hardware and Cryptanalysis

Using Normal Bases for Compact Hardware Implementations of the
 AES S-Box 236
Svetla Nikova, Vincent Rijmen, and Martin Schl affer

A New Analysis of the McEliece Cryptosystem Based on QC-LDPC
 Codes 246
Marco Baldi, Marco Bodrato, and Franco Chiaraluce

Full Cryptanalysis of LPS and Morgenstern Hash Functions 263
Christophe Petit, Kristin Lauter, and Jean-Jacques Quisquater

A New DPA Countermeasure Based on Permutation Tables 278
Jean-S bastien Coron

Session 8: Protocols II

Simplified Submission of Inputs to Protocols 293
Douglas Wikstr m

Unconditionally Reliable and Secure Message Transmission in Directed
 Networks Revisited 309
Arpita Patra, Ashish Choudhary, and C. Pandu Rangan

Session 9: Encryption III

Linear Bandwidth Naccache-Stern Encryption	327
<i>Benoît Chevallier-Mames, David Naccache, and Jacques Stern</i>	
Immunising CBC Mode against Padding Oracle Attacks: A Formal Security Treatment	340
<i>Kenneth G. Paterson and Gaven J. Watson</i>	
Constructing Strong KEM from Weak KEM (or How to Revive the KEM/DEM Framework)	358
<i>Joonsang Baek, David Galindo, Willy Susilo, and Jianying Zhou</i>	

Session 10: Key Exchange

New Anonymity Notions for Identity-Based Encryption	375
<i>Malika Izabachène and David Pointcheval</i>	
A Universally Composable Group Key Exchange Protocol with Minimum Communication Effort	392
<i>Jun Furukawa, Frederik Armknecht, and Kaoru Kurosawa</i>	
An Identity-Based Key Agreement Protocol for the Network Layer	409
<i>Christian Schridde, Matthew Smith, and Bernd Freisleben</i>	
Author Index	423