

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

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

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Carlo Blundo Stelvio Cimato (Eds.)

Security in Communication Networks

4th International Conference, SCN 2004
Amalfi, Italy, September 8-10, 2004
Revised Selected Papers



Springer

Volume Editors

Carlo Blundo

Stelvio Cimato

Università degli Studi di Salerno, Dipartimento di Informatica ed Applicazioni

84081 Baronissi (SA), Italy

E-mail: {carblu, cimato}@dia.unisa.it

Library of Congress Control Number: 2004117660

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

ISSN 0302-9743

ISBN 3-540-24301-1 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11375937 06/3142 5 4 3 2 1 0

Preface

The 4th International Conference on Security in Communication Networks 2004 (SCN 2004) was held at the “Diocese Hall” of the Archdiocese of Amalfi-Cava de’ Tirreni and the “Armorial Bearings Hall” of the Archbishop Palace in Amalfi, Italy, on September 8–10, 2004. Previous conferences also took place in Amalfi in 1996, 1999 and 2002.

The conference aimed at bringing together researchers in the fields of cryptography and security in communication networks to foster cooperation and the exchange of ideas.

The main topics included all technical aspects of data security, including: anonymity, authentication, block ciphers, complexity-based cryptography, cryptanalysis, digital signatures, distributed cryptography, hash functions, identification, implementations, key distribution, privacy, public key encryption, threshold cryptography, and zero knowledge.

The Program Committee, consisting of 21 members, considered 79 papers and selected 26 for presentation; one of them was withdrawn by the authors. These papers were selected on the basis of originality, quality and relevance to cryptography and security in communication networks.

Due to the high number of submissions, paper selection was a difficult and challenging task, and many good submissions had to be rejected. Each submission was refereed by at least three reviewers and some had four reports or more. We are very grateful to all the program committee members, who devoted much effort and valuable time to read and select the papers. In addition, we gratefully acknowledge the help of colleagues who reviewed submissions in their areas of expertise. They are all listed on page VII and we apologize for any inadvertent omissions.

These proceedings include the revised versions of the 26 accepted papers and the abstract of the invited talk by Bart Preneel (*ECRYPT: the Cryptographic Research Challenges for the Next Decade*).

Following the example of the previous editions of SCN, we encouraged authors to submit their contributions in electronic format. We handled the submissions with CyberChair (<http://www.CyberChair.org>) a free Web-based paper submission and reviewing system.

Finally, we would like to thank all the authors who submitted their papers for making this conference possible, the Program Committee members, as well as all the conference participants.

September 2004

C. Blundo
S. Cimato

Sponsoring Institutions

Dipartimento di Informatica ed Applicazioni, Università di Salerno, Italy
Lanfredi Fund, France

Referees

Michel Abdalla	Pierre-Alain Fouque	Lan Nguyen
Joonsang Baek	Clemente Galdi	Phong Nguyen
Amos Beimel	Louis Granboulan	David Pointcheval
Jan Camenisch	Matthew Green	David Safford
Claude Castelluccia	Daniel Hamburg	Willy Susilo
Dario Catalano	Jason Hinek	Nicolas Tadeusz Courtois
Xi Chen	Seny Kamara	Ivan Visconti
Qi Cheng	Aggelos Kiayias	Duncan Wong
Hung Chim	Hugo Krawczyk	Shouhuai Xu
Stelvio Cimato	TieYan Li	Jianhong Zhang
Paolo D'Arco	Becky Liu	Huafei Zhu
Breno de Medeiros	John Malone-Lee	
Xuhua Ding	Barbara Masucci	

Table of Contents

Invited Talk

ECRYPT: The Cryptographic Research Challenges for the Next Decade <i>Bart Preneel</i>	1
--	---

Reduction of Security/Primitives

Relationships Between Diffie-Hellman and “Index Oracles” <i>Adam Young, Moti Yung</i>	16
On the Security Notions for Public-Key Encryption Schemes <i>Duong Hieu Phan, David Pointcheval</i>	33
Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel <i>Claude Crépeau, Kirill Morozov, Stefan Wolf</i>	47

Signature Schemes

A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs <i>Siamak Fayyaz Shahandashti, Mahmoud Salmasizadeh, Javad Mohajeri</i>	60
Group Signatures with Separate and Distributed Authorities <i>Jun Furukawa, Shoko Yonezawa</i>	77
Threshold Cryptography for Mobile Ad Hoc Networks <i>Giovanni Di Crescenzo, Gonzalo Arce, Renwei Ge</i>	91

Anonymity and Privacy

Designated Verifier Signatures: Anonymity and Efficient Construction from <i>Any</i> Bilinear Map <i>Fabien Laguillaumie, Damien Vergnaud</i>	105
Group Signatures: Better Efficiency and New Theoretical Aspects <i>Jan Camenisch, Jens Groth</i>	120

Efficient Blind Signatures Without Random Oracles
Jan Camenisch, Maciej Koprowski, Bogdan Warinschi 134

Authentication and Identification

Minimalist Cryptography for Low-Cost RFID Tags
Ari Juels 149

On the Key Exposure Problem in Chameleon Hashes
Giuseppe Ateniese, Breno de Medeiros 165

Zero Knowledge

Identity-Based Zero Knowledge
Jonathan Katz, Rafail Ostrovsky, Michael O. Rabin 180

Public Key Cryptosystems

A Robust Multisignatures Scheme with Applications to
 Acknowledgment Aggregation
Claude Castelluccia, Stanisław Jarecki, Jihye Kim, Gene Tsudik 193

Efficient Key Encapsulation to Multiple Parties
Nigel P. Smart 208

Improved Signcryption from q -Diffie-Hellman Problems
Benoît Libert, Jean-Jacques Quisquater 220

Distributed Cryptography

Colored Visual Cryptography Without Color Darkening
Stelvio Cimato, Roberto De Prisco, Alfredo De Santis 235

On the Size of Monotone Span Programs
Ventzislav Nikov, Svetla Nikova, Bart Preneel 249

Universally Composable DKG with Linear Number of Exponentiations
Douglas Wikström 263

Cryptanalysis of Public Key Cryptosystems

An Algebraic Approach to NTRU ($q = 2^n$) via Witt Vectors and
 Overdetermined Systems of Nonlinear Equations
Joe H. Silverman, Nigel P. Smart, Frederik Vercauteren 278

Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC <i>Christopher Wolf, An Braeken, Bart Preneel</i>	294
--	-----

Cryptanalysis

The Decimated Sample Based Improved Algebraic Attacks on the Nonlinear Filters <i>Miodrag J. Mihaljević, Hideki Imai</i>	310
--	-----

Non-randomness of the Full 4 and 5-Pass HAVAL <i>Hirotaaka Yoshida, Alex Biryukov, Christophe De Cannière, Joseph Lano, Bart Preneel</i>	324
---	-----

Email Security

Controlling Spam by Secure Internet Content Selection <i>Amir Herzberg</i>	337
---	-----

Key Distribution and Feedback Shift Registers

On Session Identifiers in Provably Secure Protocols: The Bellare- Rogaway Three-Party Key Distribution Protocol Revisited <i>Kim-Kwang Raymond Choo, Colin Boyd, Yvonne Hitchcock, Greg Maitland</i>	351
--	-----

How to Embed Short Cycles into Large Nonlinear Feedback-Shift Registers <i>Le Van Ly, Werner Schindler</i>	367
--	-----

Author Index	381
---------------------------	-----