

# Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2576

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Stelvio Cimato  
Clemente Galdi  
Giuseppe Persiano (Eds.)

# Security in Communication Networks

Third International Conference, SCN 2002  
Amalfi, Italy, September 11-13, 2002  
Revised Papers



Springer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editors

Stelvio Cimato  
Giuseppe Persiano  
Università di Salerno  
Dipartimento di Informatica ed Applicazioni  
Via S. Allende, 84081 Baronissi (SA), Italy  
E-mail: {cimato/giuper}@dia.unisa.it

Clemente Galdi  
Computer Technology Institute and  
University of Patras  
Dept. of Computer Engineering and Informatics  
26500 Rio, Greece  
E-mail: clegal@ceid.upatras.gr

## Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

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 3-540-00420-3 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik  
Printed on acid-free paper SPIN: 10872336 06/3142 5 4 3 2 1 0

# Preface

The Third International Conference on Security in Communication Networks 2002 (SCN 2002) was held in the Salone Morelli of the Civic Museum of Amalfi, Italy, September 11–13, 2002. The conference takes place every three years (previous ones were held in 1996 and 1999 in Amalfi too) and aims to bring together researchers in the field of security in communication networks to foster cooperation and the exchange of ideas.

The main topics included all technical aspects of data security including: anonymity implementation, authentication, key distribution, block ciphers, operating systems security, complexity-based cryptography, privacy, cryptanalysis, protocols, digital signatures, public key encryption, electronic money, public key infrastructure, hash functions, secret sharing, identification, surveys, and the state of the art.

The program committee received 90 submissions in electronic format from 5 continents of which 24 were selected for presentation in 8 sessions. We had two invited talks, one by Eyal Kushilevitz from the Technion, Israel on “Some Applications of Polynomials for the Design of Cryptographic Protocols,” and the other by Ueli Maurer from ETH, Zurich, on “Secure Multi-Party Computation Made Simple.”

Due to the high number of submissions, the reviewing phase was a very challenging process, and many good submissions had to be rejected. We are very grateful to all the program committee members, assisted by their colleagues, who devoted much effort and valuable time to read and select the papers.

We want to thank the Municipality of Amalfi that agreed to host the conference in one of the most beautiful halls in Amalfi. Finally, we would like to thank all the authors who submitted their papers, the Program Committee members, and all the conference participants.

September 2002

S. Cimato  
C. Galdi  
G. Persiano

# Organization

SCN 2002 was organized with the financial support of the Dipartimento di Informatica ed Applicazioni “R.M. Capocelli” and the Facoltà di Scienze Matematiche, Fisiche e Naturali of the Università di Salerno under the auspices of the Amalfi Municipality.

## Program Chair

Giuseppe Persiano                      Università di Salerno, Italy

## General Chair

Carlo Blundo                              Università di Salerno, Italy

## Program Committee

Giuseppe Ateniese	(Johns Hopkins University, USA)
Carlo Blundo	(Università di Salerno, Italy)
Christian Cachin	(IBM Research, Switzerland)
Giovanni Di Crescenzo	(Telcordia Technologies, USA)
Alfredo De Santis	(Università di Salerno, Italy)
Rafail Ostrovsky	(Telcordia Technologies, USA)
Giuseppe Persiano	(Università di Salerno, Italy)
Jacques Stern	(École Normale Supérieure, France)
Doug Stinson	(University of Waterloo, Canada)
Gene Tsudik	(University of California at Irvine, USA)
Moti Yung	(Columbia University, USA)

## Organizing Committee

Stelvio Cimato	Università di Salerno, Italy
Paolo D’Arco	Università di Salerno, Italy
Clemente Galdi	Università di Salerno, Italy
Barbara Masucci	Università di Salerno, Italy

## Publicity Chairs

Vincenzo Auletta	Università di Salerno, Italy
Domenico Parente	Università di Salerno, Italy

# Table of Contents

## Invited Talks

- Some Applications of Polynomials for the Design  
of Cryptographic Protocols . . . . . 1  
*Eyal Kushilevitz (Technion)*
- Secure Multi-party Computation Made Simple . . . . . 14  
*Ueli Maurer (ETH)*

## Forward Security

- Forward Secrecy in Password-Only Key Exchange Protocols . . . . . 29  
*Jonathan Katz (University of Maryland), Rafail Ostrovsky (Telcordia  
Technologies, Inc.), and Moti Yung (Columbia University)*
- Weak Forward Security in Mediated RSA . . . . . 45  
*Gene Tsudik (University of California, Irvine)*

## Foundations of Cryptography

- On the Power of Claw-Free Permutations . . . . . 55  
*Yevgeniy Dodis (New York University)  
and Leonid Reyzin (Boston University)*
- Equivocable and Extractable Commitment Schemes . . . . . 74  
*Giovanni Di Crescenzo (Telcordia Technologies)*
- An Improved Pseudorandom Generator Based on Hardness of Factoring . . . 88  
*Nenad Dedić, Leonid Reyzin (Boston University),  
and Salil Vadhan (Harvard University)*
- Intrusion-Resilient Signatures: Generic Constructions,  
or Defeating Strong Adversary with Minimal Assumptions . . . . . 102  
*Gene Itkis (Boston University)*

## Key Management

- Efficient Re-keying Protocols for Multicast Encryption . . . . . 119  
*Giovanni Di Crescenzo (Telcordia Technologies)  
and Olga Kornievskaia (University of Michigan)*
- On a Class of Key Agreement Protocols  
Which Cannot Be Unconditionally Secure . . . . . 133  
*Frank Niedermeyer and Werner Schindler (BSI)*

A Group Key Distribution Scheme with Decentralised User Join . . . . . 146  
*Hartono Kurnio, Rei Safavi-Naini (University of Wollongong),  
and Huaxiong Wang (Macquarie University)*

## Cryptanalysis

On a Resynchronization Weakness in a Class of Combiners  
with Memory . . . . . 164  
*Yuri Borissov (Bulgarian Academy of Sciences), Svetla Nikova,  
Bart Preneel, and Joos Vandewalle (Katholieke Universiteit Leuven)*

On Probability of Success in Linear and Differential Cryptanalysis . . . . . 174  
*Ali Aydın Selçuk (Purdue University)  
and Ali Bıçak (University of Maryland Baltimore County)*

Differential Cryptanalysis of a Reduced-Round SEED . . . . . 186  
*Hitoshi Yanami and Takeshi Shimoyama (Fujitsu Laboratories LTD)*

## System Security

Medical Information Privacy Assurance:  
Cryptographic and System Aspects . . . . . 199  
*Giuseppe Ateniese, Reza Curtmola, Breno de Medeiros,  
and Darren Davis (The Johns Hopkins University)*

A *Format-Independent* Architecture for Run-Time Integrity Checking  
of Executable Code . . . . . 219  
*Luigi Catuogno and Ivan Visconti (Università di Salerno)*

## Signature Schemes

How to Repair ESIGN . . . . . 234  
*Louis Granboulan (École Normale Supérieure)*

Forward-Secure Signatures with Fast Key Update . . . . . 241  
*Anton Kozlov and Leonid Reyzin (Boston University)*

Constructing Elliptic Curves with Prescribed Embedding Degrees . . . . . 257  
*Paulo S.L.M. Barreto (Universidade de São Paulo), Ben Lynn  
(Stanford University), and Michael Scott (Dublin City University)*

A Signature Scheme with Efficient Protocols . . . . . 268  
*Jan Camenisch (IBM Research)  
and Anna Lysyanskaya (Brown University)*



## Zero Knowledge

Efficient Zero-Knowledge Proofs for Some Practical Graph Problems . . . . .	290
<i>Yvo Desmedt (Florida State University and University of London)</i> <i>and Yongge Wang (University of North Carolina at Charlotte)</i>	
Reduction Zero-Knowledge . . . . .	303
<i>Xiaotie Deng, C.H. Lee (City University of Hong Kong),</i> <i>Yunlei Zhao (City University of Hong Kong and Fudan University),</i> <i>and Hong Zhu (Fudan University)</i>	
A New Notion of Soundness in Bare Public-Key Model . . . . .	318
<i>Shirley H.C. Cheung, Xiaotie Deng, C.H. Lee (City University of Hong Kong),</i> <i>and Yunlei Zhao (City University of Hong Kong and Fudan University)</i>	

## Information Theory and Secret Sharing

Robust Information-Theoretic Private Information Retrieval . . . . .	326
<i>Amos Beimel and Yoav Stahl (Ben-Gurion University)</i>	
Trading Players for Efficiency in Unconditional Multiparty Computation . .	342
<i>B. Prabh, K. Srinathan, and C. Pandu Rangan (Indian Institute of Technology)</i>	
Secret Sharing Schemes on Access Structures with Intersection Number Equal to One . . . . .	354
<i>Jaume Martí-Farré and Carles Padró (Universitat Politècnica de Catalunya)</i>	
<b>Author Index</b> . . . . .	365