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
Preface


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The Program Committee, consisting of 21 members, considered 79 papers and selected 26 for presentation; one of them was withdrawn by the authors.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
Program Chair

Carlo Blundo
Università di Salerno, Italy

General Chair

Stelvio Cimato
Università di Salerno, Italy

Program Committee

Giuseppe Ateniese  
Johns Hopkins University, USA

Carlo Blundo  
Università di Salerno, Italy (Chair)

Christian Cachin  
IBM Research, Switzerland

Ran Canetti  
IBM Research, USA

Xiaotie Deng  
City University, Hong Kong, China

Alfredo De Santis  
Università di Salerno, Italy

Yvo Desmedt  
University College London, UK

Giovanni Di Crescenzo  
Telcordia Technology, USA

Rosario Gennaro  
IBM Research, USA

Eyal Kushilevitz  
Technion, Israel

Tanja Lange  
University of Bochum, Germany

Ueli Maurer  
ETH Zurich, Switzerland

Eiji Okamoto  
Tsukuba University, Japan

Rafail Ostrovsky  
UCLA, USA

Giuseppe Persiano  
Università di Salerno, Italy

Leonid Reyzin  
Boston University, USA

Rei Safavi-Naini  
University of Wollongong, Australia

Jacques Stern  
ENS, France

Doug Stinson  
University of Waterloo, Canada

Gene Tsudik  
UCI, USA

Moti Yung  
Columbia University, USA

Local Organizing Committee

Paolo D’Arco  
Università di Salerno, Italy

Barbara Masucci  
Università di Salerno, Italy
## Sponsoring Institutions

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

## Referees

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

Invited Talk

ECRYPT: The Cryptographic Research Challenges for the Next Decade
   Bart Preneel .................................................. 1

Reduction of Security/Primitives

Relationships Between Diffie-Hellman and “Index Oracles”
   Adam Young, Moti Yung ........................................ 16

On the Security Notions for Public-Key Encryption Schemes
   Duong Hieu Phan, David Pointcheval ........................... 33

Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel
   Claude Crépeau, Kirill Morozov, Stefan Wolf ................... 47

Signature Schemes

A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs
   Siamak Fayyaz Shahandashti, Mahmoud Salsizadeh,
   Javad Mohajeri .................................................... 60

Group Signatures with Separate and Distributed Authorities
   Jun Furukawa, Shoko Yonezawa ................................. 77

Threshold Cryptography for Mobile Ad Hoc Networks
   Giovanni Di Crescenzo, Gonzalo Arce, Renwei Ge ............ 91

Anonymity and Privacy

Designated Verifier Signatures: Anonymity and Efficient Construction from Any Bilinear Map
   Fabien Laguillaumie, Damien Vergnaud ........................ 105

Group Signatures: Better Efficiency and New Theoretical Aspects
   Jan Camenisch, Jens Groth ....................................... 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, Stanislaw 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
# Table of Contents

## Efficient Cryptanalysis of RSE(2)PKC and RSSE(2)PKC
*Christopher Wolf, An Braeken, Bart Preneel* ........................................ 294

## Cryptanalysis

The Decimated Sample Based Improved Algebraic Attacks on the Nonlinear Filters
*Miodrag J. Mihaljević, Hideki Imai* .................................................. 310

Non-randomness of the Full 4 and 5-Pass HAVAL
*Hirotaka Yoshida, Alex Biryukov, Christophe De Cannière, Joseph Lano, Bart Preneel* .................................................. 324

## Email Security

Controlling Spam by Secure Internet Content Selection
*Amir Herzberg* ................................................................. 337

## Key Distribution and Feedback Shift Registers

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

How to Embed Short Cycles into Large Nonlinear Feedback-Shift Registers
*Le Van Ly, Werner Schindler* .................................................. 367

## Author Index
* ................................................................. 381