

Lecture Notes in Computer Science

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

2384

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Lynn Batten Jennifer Seberry (Eds.)

Information Security and Privacy

7th Australasian Conference, ACISP 2002
Melbourne, Australia, July 3-5, 2002
Proceedings



Springer

Series Editors

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

Volume Editors

Lynn Batten
Deakin University, Rusden Campus
Burwood Road, Melbourne, Victoria, Australia
E-mail: lbatten@deakin.edu.au

Jennifer Seberry
University of Wollongong, Department of Computer Science
Northfields Avenue, Wollongong, NSW, Australia
E-mail: jennifer.seberry@uow.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : 7th Australasian conference ; proceedings / ACISP 2002, Melbourne, Australia, July 3 - 5, 2002. Lynn Batten ; Jennifer Seberry (ed.). - Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2384)
ISBN 3-540-43861-0

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743

ISBN 3-540-43861-0 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 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna e. K.
Printed on acid-free paper SPIN 10870504 06/3142 5 4 3 2 1 0

Preface

The Seventh Australasian Conference in Information Security and Privacy (ACISP) was held in Melbourne, 3–5 July, 2002. The conference was sponsored by Deakin University and iCORE, Alberta, Canada and the *Australian Computer Society*.

The aims of the *annual* ACISP conferences have been to bring together people working in different areas of computer, communication, and information security from universities, industry, and government institutions. The conferences give the participants the opportunity to discuss the latest developments in the rapidly growing area of information security and privacy.

The reviewing process took six weeks and we heartily thank all the members of the program committee and the external referees for the many hours of valuable time given to the conference.

The program committee accepted 36 papers from the 94 submitted. From those papers accepted 10 papers were from Australia, 5 each from Korea and USA, 4 each from Singapore and Germany, 2 from Japan, and 1 each from The Netherlands, UK, Spain, Bulgaria, and India. The authors of every paper, whether accepted or not, made a valued contribution to the conference.

In addition to the contributed papers, we were delighted to have presentations from the Victorian Privacy Commissioner, Paul Chadwick, and eminent researchers Professor Hugh Williams, Calgary, Canada, Professor Bimal Roy, ISI, Kolkota, India (whose invited talk was formally referred and accepted by the program committee), and Dr Hank Wolfe from Otago, New Zealand.

In addition we would like to thank Beom Sik Song, Willy Susilo, and especially Ken Finlayson for the vast work they put into getting this volume together in the time available.

July 2002

Lynn Batten
Jennifer Seberry

ACISP 2002

July 3-5, 2002, Melbourne, Australia

General Chair

Lynn Batten, Deakin University, Australia

Program Co-chairs

Lynn Batten, Deakin University, Australia
Jennifer Seberry, University of Wollongong, Australia

Program Committee

Colin Boyd	Queensland University of Technology, Australia
Mike Burmester	Florida State University, USA
Ed Dawson	Queensland University of Technology, Australia
Cunsheng Ding	University of Science & Technology, Hong Kong
Paul England	Microsoft, USA
Dieter Gollman	Microsoft, United Kingdom
Thomas Hardjono	VeriSign, USA
Kathy Horadam	RMIT, Australia
Kwangjo Kim	ICU, South Korea
Lars Knudsen	Technical University of Denmark, Denmark
Keith Martin	Royal Holloway, United Kingdom
Atsuko Miyaji	JAIST, Japan
Sangjae Moon	Kyungpook National University, South Korea
Yi Mu	Macquarie University, Australia
Eiji Okamoto	Toho University, Japan
Josef Pieprzyk	Macquarie University, Australia
Greg Rose	QUALCOMM, Australia
Rei Safavi-Naini	University of Wollongong, Australia
Qing Sihan	Academy of Science, China
John Snare	Adacel, Australia
Vijay Varadharajan	Macquarie University, Australia
Hugh Williams	University of Calgary, Canada
Yuliang Zheng	University of North Carolina, USA

External reviewers

Joonsang Baek, Monash University, Australia
Asha Baliga, RMIT University, Australia
Niklas Borselius, Royal Holloway, United Kingdom
Serdar Boztas, RMIT University, Australia
Laurence Bull, Monash University, Australia
Bernard Colbert, Telstra Research Laboratories, Australia
Robert Coulter, Deakin University, Australia
Ken Finlayson, Wollongong University, Australia
Goichiro Hanaoka, University of Tokyo, Japan
Marie Henderson, RMIT University, Australia
Matt Henricksen, QUT, Australia
Yvonne Hithchenson, QUT, Australia
Hartono Kurino, Wollongong University, Australia
Hiroaki Kikuchi, Japan
Jun Kogre, Fujitsu, Japan
Tanja Lange, Ruhr University, Germany
Bill Millan, QUT, Australia
Kenji Ohkuma, Toshiba, Japan
Marcus Peinado, Microsoft, USA
Ian Piper, Wollongong University, Australia
Chengxi Qu, University of New England, Australia
Matt Robshaw, Royal Holloway, United Kingdom
Nickolas Sheppard, Wollongong University, Australia
Igor Shparlinski, Macquarie University, Australia
Leonie Simpson, QUT, Australia
Masakazu Soshi, JAIST, Japan
Ron Steinfeld, Monash University, Australia
Karolyn Sprinks, Wollongong University, Australia
Willy Susilo, Wollongong University, Australia
Mitsuru Tada, Chiba University, Japan
Kapali Viswanthan, QUT, Australia
Yejing Wang, Wollongong University, Australia
Huaxiong Wang, Macquarie University, Australia
Tianbing Xia, Wollongong University, Australia
Masato Yamamichi, Japan
Jin Yuan, Hong Kong University of Science and Technology
Fanguo Zhang, ICU, Korea
Xianmo Zhang, Macquarie University, Australia

Table of Contents

Key Handling

A New Distributed Primality Test for Shared RSA Keys Using Quadratic Fields	1
<i>Ingrid Biehl, Tsuyoshi Takagi</i>	
Security Analysis and Improvement of the Global Key Recovery System ..	17
<i>Yanjiang Yang, Feng Bao, Robert H. Deng</i>	
The LILI-II Keystream Generator	25
<i>A. Clark, Ed Dawson, J. Fuller, J. Golić, H-J. Lee, William Millan, S-J. Moon, L. Simpson</i>	
A Secure Re-keying Scheme with Key Recovery Property	40
<i>Hartono Kurnio, Rei Safavi-Naini, Huaxiong Wang</i>	

Trust and Secret Sharing

Modelling Trust Structures for Public Key Infrastructures	56
<i>Marie Henderson, Robert Coulter, Ed Dawson, Eiji Okamoto</i>	
Size of Broadcast in Threshold Schemes with Disenrollment	71
<i>S.G. Barwick, W.-A. Jackson, Keith M. Martin, Peter R. Wild</i>	
Requirements for Group Independent Linear Threshold Secret Sharing Schemes	89
<i>Brian King</i>	
Efficient Sharing of Encrypted Data	107
<i>Krista Bennett, Christian Grothoff, Tzvetan Horozov, Ioana Patrascu</i>	
Cheating Prevention in Linear Secret Sharing	121
<i>Josef Pieprzyk, Xian-Mo Zhang</i>	

Fast Computation

Note on Fast Computation of Secret RSA Exponents	136
<i>Wieland Fischer, Jean-Pierre Seifert</i>	
Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying	144
<i>Leonid Reyzin, Natan Reyzin</i>	

Cryptanalysis I

Cryptanalysis of Stream Cipher COS (2, 128) Mode I	154
<i>Hongjun Wu, Feng Bao</i>	
The Analysis of Zheng-Seberry Scheme	159
<i>David Soldera, Jennifer Seberry, Chengxin Qu</i>	
Cryptanalysis of Stream Cipher Alpha1	169
<i>Hongjun Wu</i>	
A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem ...	176
<i>James Hughes</i>	

Elliptic Curves

Isomorphism Classes of Hyperelliptic Curves of Genus 2 over \mathbb{F}_q	190
<i>Y. Choie, D. Yun</i>	
Compact Representation of Domain Parameters of Hyperelliptic Curve Cryptosystems	203
<i>Fangguo Zhang, Shengli Liu, Kwangjo Kim</i>	
A New Elliptic Curve Scalar Multiplication Algorithm to Resist Simple Power Analysis	214
<i>Yvonne Hitchcock, Paul Montague</i>	

AES

Strengthening the Key Schedule of the AES	226
<i>Lauren May, Matt Henricksen, William Millan, Gary Carter, Ed Dawson</i>	
On the Necessity of Strong Assumptions for the Security of a Class of Asymmetric Encryption Schemes	241
<i>Ron Steinfeld, Joonsang Baek, Yuliang Zheng</i>	

Security Management

Security Management: An Information Systems Setting	257
<i>M.J. Warren, L.M. Batten</i>	
Resolving Conflicts in Authorization Delegations	271
<i>Chun Ruan, Vijay Varadharajan</i>	
Policy Administration Domains	286
<i>M. Hitchens, Vijay Varadharajan, G. Saunders</i>	

Authentication

- Maintaining the Validity of Digital Signatures in B2B Applications 303
Jianying Zhou
- Short 3-Secure Fingerprinting Codes for Copyright Protection 316
Francesc Sebé, Josep Domingo-Ferrer
- An Order-Specified Multisignature Scheme Secure against Active
 Insider Attacks 328
Mitsuru Tada
- Authenticated Operation of Open Computing Devices 346
Paul England, Marcus Peinado
- A New Identification Scheme Based on the Bilinear Diffie-Hellman
 Problem 362
Myungsun Kim, Kwangjo Kim

Invited Talk

- A Brief Outline of Research on Correlation Immune Functions 379
Bimal Roy

Oblivious Transfer

- m out of n Oblivious Transfer 395
Yi Mu, Junqi Zhang, Vijay Varadharajan

Cryptanalysis II

- On the Security of Reduced Versions of 3-Pass HAVAL 406
Sangwoo Park, Soo Hak Sung, Seongtaek Chee, Jongin Lim
- On Insecurity of the Side Channel Attack Countermeasure Using
 Addition-Subtraction Chains under Distinguishability between
 Addition and Doubling 420
Katsuyuki Okeya, Kouichi Sakurai
- On the Security of a Modified Paillier Public-Key Primitive 436
Kouichi Sakurai, Tsuyoshi Takagi

Dealing with Adversaries

- How to Play Sherlock Holmes in the World of Mobile Agents 449
Biljana Cubaleska, Weidong Qiu, Markus Schneider
- A Practical Approach Defeating Blackmailing 464
*Dong-Guk Han, Hye-Young Park, Young-Ho Park, Sangjin Lee,
 Dong Hoon Lee, Hyung-Jin Yang*

Privacy against Piracy: Protecting Two-Level Revocable P-K
Traitor Tracing 482
Hyun-Jeong Kim, Dong Hoon Lee, Moti Yung

Asynchronous Perfectly Secure Computation Tolerating Generalized
Adversaries 497
M.V.N. Ashwin Kumar, K. Srinathan, C. Pandu Rangan

Author Index 513