Lecture Notes in Computer Science 1587

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

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Josef Pieprzyk Rei Safavi-Naini
Jennifer Seberry (Eds.)

Information Security and Privacy

4th Australasian Conference, ACISP'99
Wollongong, NSW, Australia, April 7-9, 1999
Proceedings

Springer

Series Editors

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

Volume Editors

Josef Pieprzyk
Rei Safavi-Naini
Jennifer Seberry
University of Wollongong
School of Information Technology and Computer Science
Wollongong, NSW 2522, Australia
E-mail: {Josef_Pieprzyk, Rei_Safavi-Naini, Jennifer_Seberry}@uow.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : 4th Australasian conference ; proceedings / ACISP '99, Wollongong, NSW, Australia, April 7 - 9, 1999. Josef Pieprzyk . . . (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1587)
ISBN 3-540-65756-8

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

ISSN 0302-9743
ISBN 3-540-65756-8 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 1999
Printed in Germany

Typesetting: Camera-ready by author
SPIN: 10703993 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

The 4th Australasian Conference on Information Security and Privacy was held at the University of Wollongong, Australia. The conference was sponsored by the Centre for Computer Security Research, University of Wollongong, and the Australian Computer Society. The aim of the conference was to bring together people working in different areas of computer, communication, and information security from universities, industry, and government institutions. The conference gave the participants an opportunity to discuss the latest developments in the quickly growing area of information security and privacy.

The program committee accepted 26 papers from 53 submitted. From those accepted, thirteen papers were from Australia, two each from Belgium and China, and one each from Austria, Belarus, France, India, Japan, Korea, Singapore, the USA, and Yugoslavia. Conference sessions covered the following topics: access control and security models, network security, Boolean functions, group communication, cryptanalysis, key management systems, electronic commerce, signature schemes, RSA cryptosystems, and odds and ends.

We would like to thank the members of the program committee who generously spent their time reading and evaluating the papers. We would also like to thank members of the organising committee and, in particular, Chris Charnes, Hossein Ghodosi, Marc Gysin, Tiang-Bing Xia, Cheng-Xin Qu, San Yeow Lee, Yejing Wang, Hua-Xiong Wang, Chih-Hung Li, Willy Susilo, Chintan Shah, Jeffrey Horton, and Ghulam Rasool Chaudhry for their continuous and tireless effort in organising the conference. Finally, we would like to thank the authors of all the submitted papers, especially the accepted ones, and all the participants who made the conference a successful event.

February 1999

Josef Pieprzyk
Rei Safavi-Naini
Jennifer Seberry

FOURTH AUSTRALASIAN CONFERENCE ON INFORMATION SECURITY AND PRIVACY ACISP'99

Sponsored by

Center for Computer Security Research
University of Wollongong, Australia

and

Australian Computer Society

General Chair:

Jennifer Seberry	*University of Wollongong*

Program Co-Chairs:

Josef Pieprzyk	*University of Wollongong*
Rei Safavi-Naini	*University of Wollongong*

Program Committee:

Colin Boyd	*Queensland University of Technology, Australia*
Lawrie Brown	*Australian Defence Force Academy, Australia*
Bill Caelli	*Queensland University of Technology, Australia*
Ed Dawson	*Queensland University of Technology, Australia*
Cunsheng Ding	*National University of Singapore, Singapore*
Dieter Gollmann	*Microsoft Research, UK*
Yongfei Han	*Gemplus, Singapore*
Thomas Hardjono	*Bay Networks, US*
Erland Jonsson	*Chalmers University, Sweden*
Svein Knapskog	*University of Trondheim, Norway*
Keith Martin	*Katholieke Universiteit Leuven, Belgium*
Cathy Meadows	*Naval Research Laboratory, US*
Kaisa Nyberg	*Nokia Research Center, Finland*
Choon-Sik Park	*Electronics and Telecommunication Research Institute, Korea*
Dingyi Pei	*Academia Sinica, China*
Steve Roberts	*Witham Pty Ltd, Australia*

Greg Rose	*Qualcomm, Australia*
Ravi Sandhu	*George Mason University, US*
Stafford Tavares	*Queen's University, Canada*
Vijay Varadharajan	*Western Sydney University, Australia*
Yuliang Zheng	*Monash University, Australia*

Referees

N. Asokan
Yun Bai
Simon Blackburn
Colin Boyd
Lawrie Brown
Bill Caelli
Ed Dawson
Cunsheng Ding
Gary Gaskell
Janusz Getta
Dieter Gollmann
Marc Gysin
Yongfei Han
Thomas Hardjono
Zhang Jiang
Erland Jonsson
Svein Knapskog
Hu Lei
Leszek Maciaszek
Keith Martin
Cathy Meadows
Bill Millan
Qi Ming
Sang-Jae Moon
Yi Mu
Kenny Nguyen
Kaisa Nyberg
Choon-Sik Park
Dingyi Pei
Josef Pieprzyk
Vincent Rijmen
Steve Roberts
Greg Rose
Rei Safavi-Naini
Ravi Sandhu
Rajan Shankaran
Stafford Tavares
Vijay Varadharajan
Kapaleeswaran Viswanathan
Chuan Wu
Yuliang Zheng.

Table of Contents

Boolean Functions

Boolean Function Design Using Hill Climbing Methods
William Millan, Andrew Clark, and Ed Dawson 1

Enumeration of Correlation Immune Boolean Functions
Subhamoy Maitra and Palash Sarkar 12

On the Symmetric Property of Homogeneous Boolean Functions
Chengxin Qu, Jennifer Seberry, and Josef Pieprzyk 26

Key Management

Publicly Verifiable Key Escrow with Limited Time Span
Kapali Viswanathan, Colin Boyd, and Ed Dawson 36

Accelerating Key Establishment Protocols for Mobile Communication
Seungwon Lee, Seong-Min Hong, Hyunsoo Yoon, and Yookun Cho 51

Conference Key Agreement from Secret Sharing
Chih-Hung Li and Josef Pieprzyk 64

Cryptanalysis

On m-Permutation Protection Scheme Against Modification Attack
W.W. Fung and J.W. Gray, III 77

Inversion Attack and Branching
Jovan Dj. Golić, Andrew Clark, and Ed Dawson 88

Signatures

Fail-Stop Threshold Signature Schemes Based on Elliptic Curves
Willy Susilo, Rei Safavi-Naini, and Josef Pieprzyk 103

Divertible Zero-Knowledge Proof of Polynomial Relations and
Blind Group Signature
Khanh Quoc Nguyen, Yi Mu, and Vijay Varadharajan 117

Repudiation of Cheating and Non-repudiation of
Zhang's Proxy Signature Schemes
Hossein Ghodosi and Josef Pieprzyk 129

RSA Cryptosystems

On the Security of an RSA Based Encryption Scheme
Siguna Müller 135

Generalised Cycling Attacks on RSA and Strong RSA Primes
Marc Gysin and Jennifer Seberry 149

RSA Acceleration with Field Programmable Gate Arrays
Alexander Tiountchik and Elena Trichina 164

Group Cryptography

Changing Thresholds in the Absence of Secure Channels
Keith M. Martin, Josef Pieprzyk, Rei Safavi-Naini, and Huaxiong Wang . 177

A Self-Certified Group-Oriented Cryptosystem Without a Combiner
Shahrokh Saeednia and Hossein Ghodosi 192

Network Security

Companion Viruses and the Macintosh: Threats and Countermeasures
Jeffrey Horton and Jennifer Seberry 202

An Implementation of a Secure Version of NFS Including RBAC
Paul Ashley, Bradley Broom, and Mark Vandenwauver 213

Electronic Commerce

Group Signatures and Their Relevance to Privacy-Protecting Off-Line Electronic Cash Systems
Jacques Traoré 228

Efficient Electronic Cash Using Batch Signatures
Colin Boyd, Ernest Foo, and Chris Pavlovski 244

Evolution of Fair Non-repudiation with TTP
Jianying Zhou, Robert Deng, and Feng Bao 258

Access Control

Authorization in Object Oriented Databases
Yun Bai and Vijay Varadharajan 270

An Analysis of Access Control Models
Gregory Saunders, Michael Hitchens, and Vijay Varadharajan 281

Odds and Ends

Efficient Identity Based Parameter Selection for Elliptic Curve Cryptosystems
Arjen K. Lenstra 294

Characterization of Optimal Authentication Codes with Arbitration
Dingyi Pei, Yuqiang Li, Yejing Wang, and Rei Safavi-Naini 303

A Functional Cryptosystem Using a Group Action
Akihiro Yamamura 314

Author Index 327