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.