

Preface

The 9th Australasian Conference on Information Security and Privacy (ACISP 2004) was held in Sydney, 13–15 July, 2004. The conference was sponsored by the Centre for Advanced Computing – Algorithms and Cryptography (ACAC), Information and Networked Security Systems Research (INSS), Macquarie University and the Australian Computer Society.

The aims of the conference are to bring together researchers and practitioners working in areas of information security and privacy from universities, industry and government sectors. The conference program covered a range of aspects including cryptography, cryptanalysis, systems and network security.

The program committee accepted 41 papers from 195 submissions. The reviewing process took six weeks and each paper was carefully evaluated by at least three members of the program committee. We appreciate the hard work of the members of the program committee and external referees who gave many hours of their valuable time.

Of the accepted papers, there were nine from Korea, six from Australia, five each from Japan and the USA, three each from China and Singapore, two each from Canada and Switzerland, and one each from Belgium, France, Germany, Taiwan, The Netherlands and the UK. All the authors, whether or not their papers were accepted, made valued contributions to the conference.

In addition to the contributed papers, Dr Arjen Lenstra gave an invited talk, entitled *Likely and Unlikely Progress in Factoring*.

This year the program committee introduced the Best Student Paper Award. The winner of the prize for the Best Student Paper was Yan-Cheng Chang from Harvard University for his paper *Single Database Private Information Retrieval with Logarithmic Communication*.

We would like to thank all the people involved in organizing this conference. In particular we would like to thank members of the organizing committee for their time and efforts, Andrina Brennan, Vijayakrishnan Pasupathinathan, Har-tono Kurnio, Cecily Lenton, and members from ACAC and INSS.

July 2004

Huaxiong Wang
Josef Pieprzyk
Vijay Varadharajan

Australasian Conference on Information Security and Privacy ACISP 2004

Sponsored by

Centre for Advanced Computing – Algorithms and Cryptography (ACAC)
Information and Networked Security Systems Research (INSS)

Macquarie University
Australian Computer Society

General Chair:

Vijay Varadharajan

Macquarie University, Australia

Program Chairs:

Josef Pieprzyk

Macquarie University, Australia

Huaxiong Wang

Macquarie University, Australia

Program Committee

Feng Bao

Institute for Infocomm Research, Singapore

Lynn Batten

Deakin University, Australia

Colin Boyd

QUT, Australia

Nicolas Courtois

Axalto Smart Cards, France

Ed Dawson

QUT, Australia

Yvo Desmedt

Florida State University, USA

Cunsheng Ding

Hong Kong University of Sci. & Tech., China

Dieter Gollmann

Technical University of Hamburg, Germany

Goichiro Hanaoka

University of Tokyo, Japan

Thomas Johansson

Lund University, Sweden

Kwangjo Kim

ICU, Korea

Kaoru Kurosawa

Ibaraki Univ., Japan

Kwok-Yan Lam

Tsinghua University, China

Keith Martin

Royal Holloway, UK

Yi Mu

University of Wollongong, Australia

Christine O'Keefe

CSIRO, Australia

David Pointcheval

CNRS, France

Leonid Reyzin

Boston University, USA

Greg Rose

Qualcomm, Australia

Rei Safavi-Naini

University of Wollongong, Australia

Palash Sarkar

Indian Statistical Institute, India

Jennifer Seberry

University of Wollongong, Australia

VIII Organization

Igor Shparlinski
Doug Stinson
Hung-Min Sun
Serge Vaudenay
Chaoping Xing

Macquarie University, Australia
University of Waterloo, Canada
National Tsinghua University, Taiwan
EPFL, Switzerland
National University of Singapore, Singapore

External Referees

Mehdi-Laurent Akkar
Kazumaro Aoki
Tomoyuki Asano
Paul Ashley
Nuttapong Attrapadung
Roberto Avanzi
Gildas Avoine
Thomas Baigneres
Emmanuel Bresson
Dario Catalano
Sanjit Chatterjee
Chien-Ning Chen
Ling-Hwei Chen
Xiaofeng Chen
Bo-Chao Cheng
Chi-Hung Chi
Joo Yeon Cho
Siu-Leung Chung
Andrew Clark
Scott Contini
Don Coppersmith
Yang Cui
Tanmoy Kanti Das
Alex Dent
Christophe Doche
Ratna Dutta
Chun-I Fan
Serge Fehr
Ernest Foo
Pierre-Alain Fouque
Jun Furukawa
Rosario Gennaro
Juanma Gonzalez-Nieto
Louis Goubin
Zhi Guo
Philip Hawkes
Martin Hell

Matt Henricksen
Shoichi Hirose
Yvonne Hitchcock
Chiou-Ting Hsu
Min-Shiang Hwang
Gene Itkis
Toshiya Itoh
Tetsu Iwata
Marc Joye
Pascal Junod
Byoungcheon Lee
Yan-Xia Lin
Der-Chyuan Lou
Chi-Jen Lu
Stefan Lucks
Phil MacKenzie
Subhamoy Maitra
Cecile Malinaud
Tal Malkin
Wenbo Mao
Thomas Martin
Tatsuyuki Matsushita
Toshihiro Matsuo
Luke Mcaven
Robert McNerney
Tom Messerges
Pradeep Kumar Mishra
Chris Mitchell
Jean Monnerat
Joern Mueller-Quade
James Muir
Seiji Munetoh
Sean Murphy
Anderson Nascimento
Lan Ngyuen
Phong Nguyen
Philippe Oechslin

Miyako Ohkubo
Yasuhiro Ohtaki
Wakaha Ogata
Michael Paddon
Doug Palmer
Jacques Patarin
Kenny Paterson
Kun Peng
Krzysztof Pietrzak
Angela Piper
Jason Reid
Ryuichi Sakai
Renate Scheidler
Nichoas Sheppard
SeongHan Shin
Leonie Simpson
Hong-Wei Sun
Willy Susilo
Isamu Teranishi
Dong To
Woei-Jiunn Tsaur
Din-Chang Tseng
Takeyuki Uehara
David Wagner
Chih-Hung Wang
William Whyte
Hongjun Wu
Tzong-Chen Wu
Sung-Ming Yen
Lu Yi
Takuya Yoshida
Ming Yung
Moti Yung
Fangguo Zhang
Rui Zhang
Xi-Bin Zhao

Information Security and Privacy

9th Australasian Conference, ACISP 2004, Sydney,
Australia, July 13-15, 2004, Proceedings

Wang, H.; Pieprzyk, J.; Varadharajan, V. (Eds.)

2004, XIV, 498 p., Softcover

ISBN: 978-3-540-22379-5