

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Huaxiong Wang Josef Pieprzyk
Vijay Varadharajan (Eds.)

Information Security and Privacy

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



Springer

Volume Editors

Huaxiong Wang
Josef Pieprzyk
Vijay Varadharajan
Macquarie University
Department of Computing
Sydney, NSW 2109, Australia
E-mail: {hwang,josef,vijay}@ics.mq.edu.au

Library of Congress Control Number: 2004108445

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 3-540-22379-7 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 to prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11019282 06/3142 5 4 3 2 1 0

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

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 McNeerney
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 Tsauro
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

Table of Contents

Broadcast Encryption and Traitor Tracing

Multi-service Oriented Broadcast Encryption	1
<i>Shaoquan Jiang, Guang Gong</i>	
Secure and Insecure Modifications of the Subset Difference Broadcast Encryption Scheme	12
<i>Tomoyuki Asano</i>	
Linear Code Implies Public-Key Traitor Tracing With <i>Revocation</i>	24
<i>Vu Dong Tô, Reihaneh Safavi-Naini</i>	
TTS Without Revocation Capability Secure Against CCA2	36
<i>Chong Hee Kim, Yong Ho Hwang, Pil Joong Lee</i>	

Private Information Retrieval and Oblivious Transfer

Single Database Private Information Retrieval With Logarithmic Communication	50
<i>Yan-Cheng Chang</i>	
Information Theoretically Secure Oblivious Polynomial Evaluation: Model, Bounds, and Constructions	62
<i>Goichiro Hanaoka, Hideki Imai, Joern Mueller-Quade, Anderson C.A. Nascimento, Akira Otsuka, Andreas Winter</i>	

Trust and Secret Sharing

Optimistic Fair Exchange Based on Publicly Verifiable Secret Sharing	74
<i>Gildas Avoine, Serge Vaudenay</i>	
NGSCB: A Trusted Open System	86
<i>Marcus Peinado, Yuqun Chen, Paul England, John Manferdelli</i>	

Cryptanalysis (I)

The Biryukov-Demirci Attack on Reduced-Round Versions of IDEA and MESH Ciphers	98
<i>Jorge Nakahara, Jr., Bart Preneel, Joos Vandewalle</i>	

Differential-Linear Type Attacks on Reduced Rounds of SHACAL-2	110
<i>Yongsup Shin, Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee</i>	
The Related-Key Rectangle Attack – Application to SHACAL-1	123
<i>Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee, Dowon Hong</i>	
Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1	137
<i>Youngdai Ko, Changhoon Lee, Seokhie Hong, Sangjin Lee</i>	
The Security of Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders	149
<i>Michael J. Jacobson, Jr.</i>	
Cryptanalysis (II)	
Analysis of a Conference Scheme Under Active and Passive Attacks	157
<i>Feng Bao</i>	
Cryptanalysis of Two Password-Authenticated Key Exchange Protocols	164
<i>Zhiguo Wan, Shuhong Wang</i>	
Analysis and Improvement of Micali's Fair Contract Signing Protocol	176
<i>Feng Bao, Guilin Wang, Jianying Zhou, Huafei Zhu</i>	
Digital Signatures (I)	
Digital Signature Schemes With Domain Parameters	188
<i>Serge Vaudenay</i>	
Generic Construction of Certificateless Signature	200
<i>Dae Hyun Yum, Pil Joong Lee</i>	
Cryptosystems (I)	
A Generalization of PGV-Hash Functions and Security Analysis in Black-Box Model	212
<i>Wonil Lee, Mridul Nandi, Palash Sarkar, Donghoon Chang, Sangjin Lee, Kouichi Sakurai</i>	
How to Re-use Round Function in Super-Pseudorandom Permutation	224
<i>Tetsu Iwata, Kaoru Kurosawa</i>	
How to Remove MAC from DHIES	236
<i>Kaoru Kurosawa, Toshihiko Matsuo</i>	

Symmetric Key Authentication Services Revisited	248
<i>Bruno Crispo, Bogdan C. Popescu, Andrew S. Tanenbaum</i>	

Fast Computation

Improvements to the Point Halving Algorithm	262
<i>Brian King, Ben Rubin</i>	
Theoretical Analysis of XL over Small Fields	277
<i>Bo-Yin Yang, Jiun-Ming Chen</i>	
A New Method for Securing Elliptic Scalar Multiplication Against Side-Channel Attacks	289
<i>Chae Hoon Lim</i>	

Mobile Agents Security

A Mobile Agent System Providing Offer Privacy	301
<i>Ming Yao, Matt Henricksen, Greg Maitland, Ernest Foo, Ed Dawson</i>	

Digital Signatures (II)

Identity-Based Strong Designated Verifier Signature Schemes	313
<i>Willy Susilo, Fangguo Zhang, Yi Mu</i>	
Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups	325
<i>Joseph K. Liu, Victor K. Wei, Duncan S. Wong</i>	
A Group Signature Scheme With Efficient Membership Revocation for Reasonable Groups	336
<i>Toru Nakanishi, Yuji Sugiyama</i>	
Convertible Nominative Signatures	348
<i>Zhenjie Huang, Yumin Wang</i>	

Protocols

Protocols With Security Proofs for Mobile Applications	358
<i>Yiu Shing Terry Tin, Harikrishna Vasanta, Colin Boyd, Juan Manuel González Nieto</i>	
Secure Bilinear Diffie-Hellman Bits	370
<i>Steven D. Galbraith, Herbie J. Hopkins, Igor E. Shparlinski</i>	
Weak Property of Malleability in NTRUSign	379
<i>SungJun Min, Go Yamamoto, Kwangjo Kim</i>	

Security Management

Information Security Risk Assessment, Aggregation, and Mitigation 391
Arjen Lenstra, Tim Voss

Access Control and Authorisation

A Weighted Graph Approach
to Authorization Delegation and Conflict Resolution..... 402
Chun Ruan, Vijay Varadharajan

Authorization Mechanisms for Virtual Organizations
in Distributed Computing Systems 414
*Xi-Bin Zhao, Kwok-Yan Lam, Siu-Leung Chung, Ming Gu,
Jia-Guang Sun*

Cryptosystems (II)

Unconditionally Secure Encryption Under Strong Attacks 427
Luke McAven, Rei Safavi-Naini, Moti Yung

ManTiCore: Encryption With Joint Cipher-State Authentication..... 440
*Erik Anderson, Cheryl Beaver, Timothy Draelos,
Richard Schroepel, Mark Torgerson*

Cryptanalysis (III)

On Security of XTR Public Key Cryptosystems
Against Side Channel Attacks 454
Dong-Guk Han, Jongin Lim, Kouichi Sakurai

On the Exact Flexibility of the Flexible Countermeasure
Against Side Channel Attacks 466
Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume

Fault Attacks on Signature Schemes 478
Christophe Giraud, Erik W. Knudsen

Author Index 493