

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

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

University of California, Los Angeles, CA, 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

Josef Pieprzyk Hossein Ghodosi
Ed Dawson (Eds.)

Information Security and Privacy

12th Australasian Conference, ACISP 2007
Townsville, Australia, July 2-4, 2007
Proceedings

Volume Editors

Josef Pieprzyk

Macquarie University, Department of Computing
Center for Advanced Computing - Algorithms and Cryptography
Sydney, NSW 2109, Australia
E-mail: josef@ics.mq.edu.au

Hossein Ghodosi

James Cook University
School of Mathematics, Physics, and Information Technology
Townsville, QLD 4811, Australia
E-mail: hossein@cs.jcu.edu.au

Ed Dawson

Queensland University of Technology, Information Security Institute
Brisbane, QLD 4001, Australia
E-mail: e.dawson@qut.edu.au

Library of Congress Control Number: 2007929635

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-73457-0 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-73457-4 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12086818 06/3180 5 4 3 2 1 0

Preface

The 12th Australasian Conference on Information Security and Privacy—ACISP2007—was held in Townsville, Queensland, July 2–4, 2007. This was the first conference to be organized outside the traditional three venues: Brisbane and Gold Coast, Melbourne, and Sydney and Wollongong. The conference was sponsored by James Cook University, Center for Advanced Computing – Algorithm and Cryptography at Macquarie University, Information Security Institute at Queensland University of Technology, and the Research Network for Secure Australia. We would like to thank Matthieu Finiasz and Thomas Baignères from EPFL, LASEC, Switzerland for letting us use their iChair software that facilitated the submission and revision processes.

Out of 132 submissions, the Program Committee (PC) selected 33 papers after a rigorous review process. Each paper got assigned to at least three referees. Papers submitted by members of the PC got assigned to five referees. In the first stage of the review process, the submitted papers were read and evaluated by the PC members and then in the second stage, the papers were scrutinized during a three-week-long discussion. We would like to thank the authors of all papers (both accepted and rejected) for submitting their papers to the conference. A special thanks go to the members of the PC and the external referees who gave their time, expertise and enthusiasm in order to select the best collection of papers.

As in previous years, we held a competition for the “best student paper.” To be eligible, a paper had to be co-authored by a postgraduate student whose contribution was more than 50%. Eight papers entered the competition. The winner was Norbert Pramstaller from Graz University of Technology, Austria, for the paper “Second Preimages for Iterated Hash Functions and Their Implications on MACs.”

This year we had only one invited talk, which was given by Andreas Enge. The title of the talk was “Contributions Cryptographic Curves.”

We would like to express our thanks to Springer and in particular, to Alfred Hofmann and Ronan Nugent for their continuing support of the ACISP conference and for help in the conference proceeding production. Further, we thank Michelle Kang, who helped us with the setting up and maintenance of the ACISP Web site, Vijayakrishnan Pasupathinathan, who took care of the iChair server and ACISP mailbox, Adam Shah for installation of the iChair server and Elizabeth Hansford for assisting with conference organization.

July 2007

Josef Pieprzyk
Hossein Ghodosi
Ed Dawson

Organization

ACISP 2007

July 2–4, 2007, Townsville, Queensland, Australia

General Co-chairs

Hossein Ghodosi	James Cook University, Australia
Ed Dawson	QUT, Australia

Program Chair

Josef Pieprzyk	Macquarie University, Australia
----------------	---------------------------------

Program Committee

Paul Ashley	IBM, Australia
Tuomas Aura	Microsoft, USA
Lynn Batten	Deakin University, Australia
Colin Boyd	QUT, Australia
Andrew Clark	QUT, Australia
Scott Contini	Macquarie University, Australia
Nicolas Courtois	University College London, UK and Gemalto, France
Yvo Desmedt	University College London, UK
Christophe Doche	Macquarie University, Australia
Ed Dawson	QUT, Australia
Hossein Ghodosi	James Cook University, Australia
Jovan Golić	Telecom, Italy
Dieter Gollmann	TUHH, Germany
Peter Gutmann	University of Auckland, New Zealand
Kwangjo Kim	ICU, Korea
Sevin Knapskog	NTNU, Norway
Kaoru Kurosawa	Ibaraki University, Japan
Tanja Lange	TU/e, Netherlands
Javier Lopez	University of Malaga, Spain
Keith Martin	Royal Holloway, UK
Mitsuru Matsui	Mitsubishi Electric, Japan
Paul Montague	Motorola, Australia
Yi Mu	University of Wollongong, Australia
Andrew Odlyzko	University of Minnesota, USA
Eiji Okamoto	University of Tsukuba, Japan
Rafail Ostrovsky	UCLA, USA

David Poincheval	ENS, France
Bart Preneel	K.U.Leuven, Belgium
Bimal Roy	ISICAL, India
Rei Safavi-Naini	University of Wollongong, Australia
	University of Calgary, Canada
Jennifer Seberry	University of Wollongong, Australia
Igor Shparlinski	Macquarie University, Australia
Ron Steinfeld	Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Henk van Tilborg	TU/e, Netherlands
Serge Vaudenay	EPFL, Switzerland
Huaxiong Wang	Macquarie University, Australia
	Nanyang Technological University, Singapore
Henry Wolfe	University of Otago, New Zealand

External Reviewers

Ajith Abraham	Avishek Adhikari	Isaac Agudo
Man Ho Au	Joonsang Baek	Vittorio Bagini
Yun Bai	Thomas Baignères	Rana Barua
Daniel J. Bernstein	Peter Birkner	Xavier Boyen
Yang Cui	Jan Camenisch	Christophe De Cannière
Alvaro Cardenas	Dario Catalano	Agnes Chan
Chris Charnes	Benoit Chevallier-Mames	Sherman S. M. Chow
Yvonne Cliff	Tanmoy Das	Pascal Delaunay
Dang Nguyen Duc	Ernest Foo	Pierre-Alain Fouque
Jun Furukawa	Krzysztof M. Gaj	David Galindo
Juan Garay	Danilo Gligoroski	M. Choudary Gorantla
Jens Groth	Kishan Chand Gupta	Goichiro Hanaoka
Kjetil Haslum	Swee-Huay Heng	Jonathan Herzog
Shoichi Hirose	Michael Hitchens	Jeffrey Horton
Xinyi Huang	Laurent Imbert	Sebastiaan Indesteege
Mahabir Prasad Jhanwar	Emilia Käsper	Lars R. Knudsen
Markulf Kohlweiss	Divyan M. Konidala	Takeshi Koshiha
Kerstin Lemke-Rust	Vo Duc Liem	Chu-Wee Lim
Liang Liu	Liang Lu	Anna Lysyanskaya
Mark Manulis	Abe Masayuki	Krystian Matusiewicz
Luke McAven	Miodrag Mihaljevic	Ilya Mironov
Guglielmo Morgari	Sean Murphy	Pablo Najera
Gregory Neven	Antonio Nicolosi	Svetla Nikova
Wakaha Ogata	Jose A. Onieva	Dunkelman Orr
Pascal Paillier	Sylvain Pasini	Kenny Paterson
Maura Paterson	Goutam Paul	Souradyuti Paul
Kun Peng	Slobodan Petrovic	Raphael C.-W. Phan
Le Trieu Phong	Geraint Price	Havard Raddum

Mohammad Reza Reyhanitabar	Rodrigo Roman	Greg Rose
Chun Ruan	Yasuyuki Sakai	Somitra Sanadhya
Siamak Shahandashti	Nicholas Sheppard	Jason Smith
Makoto Sugita	Daisuke Suzuki	Katsuyuki Takashima
Qiang Tang	Christophe Tartary	Clark Thomborson
Toshio Tokita	Jacques Traore	Pim Tuyls
Frederik Vercauteren	Charlotte Vikkelsoe	Martin Vuagnoux
Guilin Wang	Peishun Wang	Shuhong Wang
Yan Wang	Yongge Wang	Brent Waters
Benne de Weger	Christopher Wolf	Hongjun Wu
Qianhong Wu	Guangwu Xu	Bo-Yin Yang
Qingsong Ye	Hongbo Yu	Steve Zdancewic
Sébastien Zimmer		

Table of Contents

Stream Ciphers

An Analysis of the Hermes8 Stream Ciphers	1
<i>Steve Babbage, Carlos Cid, Norbert Pramstaller, and Håvard Raddum</i>	
On the Security of the LILI Family of Stream Ciphers Against Algebraic Attacks	11
<i>Sultan Zayid Al-Hinai, Ed Dawson, Matt Henricksen, and Leonie Simpson</i>	
Strengthening NLS Against Crossword Puzzle Attack	29
<i>Debojyoti Bhattacharya, Debdeep Mukhopadhyay, Dhiman Saha, and D. RoyChowdhury</i>	

Hashing

A New Strategy for Finding a Differential Path of SHA-1	45
<i>Jun Yajima, Yu Sasaki, Yusuke Naito, Terutoshi Iwasaki, Takeshi Shimoyama, Noboru Kunihiro, and Kazuo Ohta</i>	
Preimage Attack on the Parallel FFT-Hashing Function	59
<i>Donghoon Chang, Moti Yung, Jaechul Sung, Seokhie Hong, and Sangjin Lee</i>	
Second Preimages for Iterated Hash Functions and Their Implications on MACs	68
<i>Norbert Pramstaller, Mario Lamberger, and Vincent Rijmen</i>	
On Building Hash Functions from Multivariate Quadratic Equations . . .	82
<i>Olivier Billet, Matt J.B. Robshaw, and Thomas Peyrin</i>	

Biometrics

An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication	96
<i>Julien Bringer, Hervé Chabanne, Malika Izabachène, David Pointcheval, Qiang Tang, and Sébastien Zimmer</i>	
Soft Generation of Secure Biometric Keys	107
<i>Jovan Dj. Golić and Madalina Baltatu</i>	

Secret Sharing

Flaws in Some Secret Sharing Schemes Against Cheating	122
<i>Toshinori Araki and Satoshi Obana</i>	

Efficient (k, n) Threshold Secret Sharing Schemes Secure Against Cheating from $n - 1$ Cheaters	133
<i>Toshinori Araki</i>	

Cryptanalysis

Related-Key Amplified Boomerang Attacks on the Full-Round Eagle-64 and Eagle-128	143
<i>Kitae Jeong, Changhoon Lee, Jaechul Sung, Seokhie Hong, and Jongin Lim</i>	
Analysis of the SMS4 Block Cipher	158
<i>Fen Liu, Wen Ji, Lei Hu, Jintai Ding, Shuwang Lv, Andrei Pyshkin, and Ralf-Philipp Weinmann</i>	
Forgery Attack to an Asymptotically Optimal Traitor Tracing Scheme	171
<i>Yongdong Wu, Feng Bao, and Robert H. Deng</i>	

Public Key Cryptography

TCHo : A Hardware-Oriented Trapdoor Cipher	184
<i>Jean-Philippe Aumasson, Matthieu Finiasz, Willi Meier, and Serge Vaudenay</i>	
Anonymity on Paillier's Trap-Door Permutation	200
<i>Ryotaro Hayashi and Keisuke Tanaka</i>	
Generic Certificateless Key Encapsulation Mechanism	215
<i>Qiong Huang and Duncan S. Wong</i>	
Double-Size Bipartite Modular Multiplication	230
<i>Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume</i>	
Affine Precomputation with Sole Inversion in Elliptic Curve Cryptography	245
<i>Erik Dahmen, Katsuyuki Okeya, and Daniel Schepers</i>	
Construction of Threshold (Hybrid) Encryption in the Random Oracle Model: How to Construct Secure Threshold Tag-KEM from Weakly Secure Threshold KEM	259
<i>Takeru Ishihara, Hiroshi Aono, Sadayuki Hongo, and Junji Shikata</i>	
Efficient Chosen-Ciphertext Secure Identity-Based Encryption with Wildcards	274
<i>James Birkett, Alexander W. Dent, Gregory Neven, and Jacob C.N. Schuldt</i>	

Authentication

Combining Prediction Hashing and MDS Codes for Efficient Multicast Stream Authentication	293
<i>Christophe Tartary and Huaxiong Wang</i>	
Certificateless Signature Revisited	308
<i>Xinyi Huang, Yi Mu, Willy Susilo, Duncan S. Wong, and Wei Wu</i>	
Identity-Committable Signatures and Their Extension to Group-Oriented Ring Signatures	323
<i>Cheng-Kang Chu and Wen-Guey Tzeng</i>	
Hash-and-Sign with Weak Hashing Made Secure	338
<i>Sylvain Pasini and Serge Vaudenay</i>	
“Sandwich” Is Indeed Secure: How to Authenticate a Message with Just One Hashing	355
<i>Kan Yasuda</i>	
Threshold Anonymous Group Identification and Zero-Knowledge Proof	370
<i>Akihiro Yamamura, Takashi Kurokawa, and Junji Nakazato</i>	
Non-interactive Manual Channel Message Authentication Based on eTCR Hash Functions	385
<i>Mohammad Reza Reyhanitabar, Shuhong Wang, and Reihaneh Safavi-Naini</i>	

E-Commerce

A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users	400
<i>Stefan Brands, Liesje Demuyne, and Bart De Decker</i>	
Efficient and Secure Comparison for On-Line Auctions	416
<i>Ivan Damgård, Martin Geisler, and Mikkel Krøigaard</i>	
Practical Compact E-Cash	431
<i>Man Ho Au, Willy Susilo, and Yi Mu</i>	

Security

Use of Dempster-Shafer Theory and Bayesian Inferencing for Fraud Detection in Mobile Communication Networks	446
<i>Suvasini Panigrahi, Amlan Kundu, Shamik Sural, and A.K. Majumdar</i>	

On Proactive Perfectly Secure Message Transmission 461
 Kannan Srinathan, Prasad Raghavendra, and
 Pandu Rangan Chandrasekaran

Author Index 475