

Ron Steinfeld Philip Hawkes (Eds.)

# Information Security and Privacy

15th Australasian Conference, ACISP 2010  
Sydney, Australia, July 5-7, 2010  
Proceedings

## Volume Editors

Ron Steinfeld  
Macquarie University, Department of Computing  
North Ryde, NSW 2109, Australia  
E-mail: rons@science.mq.edu.au

Philip Hawkes  
Qualcomm Incorporated  
Suite 301, Level 3, 77 King Street, Sydney, NSW 2000, Australia  
E-mail: phawkes@qualcomm.com

Library of Congress Control Number: 2010929205

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, J.1, G.2.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743  
ISBN-10 3-642-14080-7 Springer Berlin Heidelberg New York  
ISBN-13 978-3-642-14080-8 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.com

© Springer-Verlag Berlin Heidelberg 2010  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper 06/3180

# Preface

The annual Australasian Conference on Information Security and Privacy is the premier Australian academic conference in its field, showcasing research from around the globe on a range of topics. ACISP 2010 was held during July 5-7, 2010, at Macquarie University in Sydney, Australia.

There were 97 paper submissions for the conference. These submissions were reviewed by the Program Committee and a number of other individuals, whose names can be found overleaf. The Program Committee then selected 24 papers for presentation at the conference. These papers are contained in these proceedings.

In addition to the peer-reviewed papers, two invited speakers presented talks at the conference: Craig Gentry (IBM, USA); and Stephan Overbeek (Shearwater Solutions, Australia). We would like to express our gratitude to Craig and Stephan for contributing their knowledge and insight, and thus expanding the horizons of the conference delegates.

We would like to thank the authors of all of the submissions for offering their research for publication in ACISP 2010. We extend our sincere thanks to the Program Committee and other reviewers for the high-quality reviews and in-depth discussion. The Program Committee made use of the iChair electronic submission and reviewing software written by Thomas Baignères and Matthieu Finiasz at EPFL, LASEC. We would like to express our thanks to Springer for continuing to support the ACISP conference and for help in the conference proceedings production. We also thank the Organizing Committee, led by the ACISP 2010 General Chair Josef Pieprzyk, for their contribution to the conference.

Finally, we would like to thank our sponsors, iRobot, and our hosts, Qualcomm Inc. and the Centre for Advanced Computing - Algorithms and Cryptography (ACAC) at Macquarie University.

July 2010

Ron Steinfeld  
Philip Hawkes

# Organization

## General Chair

Josef Pieprzyk

Macquarie University, Australia

## Program Co-chairs

Ron Steinfeld

Macquarie University, Australia

Philip Hawkes

Qualcomm Incorporated, Australia

## Program Committee

Michel Abdalla

École Normale Supérieure, France

Masayuki Abe

NTT, Japan

Magnus Almgren

Chalmers University of Technology, Sweden

Joonsang Baek

Institute for Infocomm Research, Singapore

Feng Bao

Institute for Infocomm Research, Singapore

Lynn Batten

Deakin University, Australia

Alex Biryukov

University of Luxembourg, Luxembourg

Colin Boyd

Queensland University of Technology, Australia

Joo Yeon Cho

Nokia A/S, Denmark

Carlos Cid

Royal Holloway, University of London, UK

Andrew Clark

Queensland University of Technology, Australia

Nicolas Courtois

University College London, UK

Yvo Desmedt

University College London, UK and RCIS,  
AIST, Japan

Christophe Doche

Macquarie University, Australia

Ulrich Flegel

SAP Research, Germany

Steven Galbraith

University of Auckland, New Zealand

Juan Gonzalez Nieto

Queensland University of Technology, Australia

Maria Isabel Gonzalez Vasco

Universidad Rey Juan Carlos, Spain

Peter Gutmann

University of Auckland, New Zealand

Svein Knapskog

Norwegian University of Science and  
Technology, Norway

Xuejia Lai

Shanghai Jiao Tong University, China

Mark Manulis

TU Darmstadt, Germany

Keith Martin

Royal Holloway, University of London, UK

Mitsuru Matsui

Mitsubishi Electric, Japan

Krystian Matuiesewicz

Technical University of Denmark, Denmark

Chris Mitchell

Royal Holloway, University of London, UK

Atsuko Miyaji

JAIST, Japan

Yi Mu	University of Wollongong, Australia
C. Pandu Rangan	IIT, Madras, India
Vincent Rijmen	KU Leuven, Belgium and TU Graz, Austria
Rei Safavi Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Berry Schoenmakers	TU Eindhoven, The Netherlands
Jennifer Seberry	University of Wollongong, Australia
Damien Stehlé	CNRS, France and University of Sydney, Australia and Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Serge Vaudenay	EPFL, Switzerland
Damien Vergnaud	École Normale Supérieure, France
Huaxiong Wang	Nanyang Technological University, Singapore and Macquarie University, Australia
Duncan Wong	City University of Hong Kong, Hong Kong
Kan Yasuda	NTT, Japan
Yuliang Zheng	University of North Carolina at Charlotte, USA

## External Reviewers

Hadi Ahmadi	Jialin Huang	Kaisa Nyberg
Man Ho Au	Qiong Huang	Tomas Olovsson
Gleb Beliakov	Ralf Hund	Kazumasa Omote
Simon R. Blackburn	Shaoquan Jiang	Khaled Ouafi
Thomas Bläsing	Charanjit Jutla	Vijayakrishnan
Jens-Matthias Bohli	Dmitry Khovratovich	Pasupathinathan
Ignacio Cascudo	Andreas Larsson	Serdar Pehlivanoglu
Rafik Chaabouni	Pho Le	Henning Rogge
Xiaofeng Chen	Gregor Leander	Markus Rueckert
Zhengjie Cheng	Benoit Libert	Minoru Saeki
Cline Chevalier	Tingting Lin	Yu Sasaki
Sebastian de Hoogh	Joseph K. Liu	Takashi Satoh
Georg Fuchsbauer	Shengli Liu	Jacob Schuldt
Jun Furukawa	Yi Lu	Sharmila Deva Selvi
Martin Gagne	Yiyuan Luo	Pouyan Sepehrdad
Choudary Gorantla	Takahiro Matsuda	Siamak F. Shahandashti
Vipul Goyal	Florian Mendel	Masaaki Shirase
Jian Guo	Ivan Morel	Magnus Själander
Fuchun Guo	Sumio Morioka	Benjamin Smith
Hua Guo	Sean Murphy	Boyeon Song
Gerhard Hancke	Jorge Nakahara Jr	Suriadi Suriadi
Javier Herranz	Kris Narayan	Daisuke Suzuki
Fumitaka Hoshino	Andrew Novocin	Christophe Tartary
Xinyi Huang	Attrapadung Nuttapong	Alan Tickle

Ashrafal Tuhin  
Oriol FARRS Ventura  
Jorge Luis Villar  
Ulrich Vollmer  
Christian Wachsmann  
Yan Wang

Guilin Wang  
Peishun Wang  
Benne de Weger  
Puwen Wei  
Ralf-Philipp Weinmann  
Andrew White

Wei Wu  
Yongdong Wu  
Guomin Yang  
Po-Wah Yau  
Tsz Hon Yuen  
Huafei Zhu

# Table of Contents

## Symmetric Key Encryption

Cryptanalysis of a Generalized Unbalanced Feistel Network Structure . . .	1
<i>Ruilin Li, Bing Sun, Chao Li, and Longjiang Qu</i>	
Improved Algebraic Cryptanalysis of QUAD, Bivium and Trivium via Graph Partitioning on Equation Systems . . . . .	19
<i>Kenneth Koon-Ho Wong and Gregory V. Bard</i>	
On Multidimensional Linear Cryptanalysis . . . . .	37
<i>Phuong Ha Nguyen, Lei Wei, Huaxiong Wang, and San Ling</i>	
Side-Channel Analysis of the K2 Stream Cipher . . . . .	53
<i>Matt Henricksen, Wun She Yap, Chee Hoo Yian, Shinsaku Kiyomoto, and Toshiaki Tanaka</i>	
On Unbiased Linear Approximations . . . . .	74
<i>Jonathan Etrog and Matthew J.B. Robshaw</i>	

## Hash Functions

Distinguishers for the Compression Function and Output Transformation of Hamsi-256 . . . . .	87
<i>Jean-Philippe Aumasson, Emilia Käster, Lars Ramkilde Knudsen, Krystian Matusiewicz, Rune Ødegård, Thomas Peyrin, and Martin Schläffer</i>	
Second-Preimage Analysis of Reduced SHA-1 . . . . .	104
<i>Christian Rechberger</i>	
Some Observations on Indifferentiability . . . . .	117
<i>Ewan Fleischmann, Michael Gorski, and Stefan Lucks</i>	

## Public Key Cryptography

Adaptive and Composable Non-committing Encryptions . . . . .	135
<i>Huafei Zhu, Tadashi Araragi, Takashi Nishide, and Kouichi Sakurai</i>	
Relations among Notions of Complete Non-malleability: Indistinguishability Characterisation and Efficient Construction without Random Oracles . . . . .	145
<i>Manuel Barbosa and Pooya Farshim</i>	
Strong Knowledge Extractors for Public-Key Encryption Schemes . . . . .	164
<i>Manuel Barbosa and Pooya Farshim</i>	

A Multi-trapdoor Commitment Scheme from the RSA Assumption . . . . .	182
<i>Ryo Nishimaki, Eiichiro Fujisaki, and Keisuke Tanaka</i>	
Identity-Based Chameleon Hash Scheme without Key Exposure . . . . .	200
<i>Xiaofeng Chen, Fanguo Zhang, Willy Susilo, Haibo Tian, Jin Li, and Kwangjo Kim</i>	
The Security Model of Unidirectional Proxy Re-Signature with Private Re-Signature Key . . . . .	216
<i>Jun Shao, Min Feng, Bin Zhu, Zhenfu Cao, and Peng Liu</i>	
Security Estimates for Quadratic Field Based Cryptosystems . . . . .	233
<i>Jean-François Biasse, Michael J. Jacobson Jr., and Alan K. Silvester</i>	
Solving Generalized Small Inverse Problems . . . . .	248
<i>Noboru Kunihiro</i>	
<b>Protocols</b>	
One-Time-Password-Authenticated Key Exchange . . . . .	264
<i>Kenneth G. Paterson and Douglas Stebila</i>	
Predicate-Based Key Exchange . . . . .	282
<i>James Birkett and Douglas Stebila</i>	
Attribute-Based Authenticated Key Exchange . . . . .	300
<i>M. Choudary Gorantla, Colin Boyd, and Juan Manuel González Nieto</i>	
Optimally Tight Security Proofs for Hash-Then-Publish Time-Stamping . . . . .	318
<i>Ahto Buldas and Margus Nüitsoo</i>	
Additive Combinatorics and Discrete Logarithm Based Range Protocols . . . . .	336
<i>Rafik Chaabouni, Helger Lipmaa, and Abhi Shelat</i>	
Proof-of-Knowledge of Representation of Committed Value and Its Applications . . . . .	352
<i>Man Ho Au, Willy Susilo, and Yi Mu</i>	
<b>Network Security</b>	
Pattern Recognition Techniques for the Classification of Malware Packers . . . . .	370
<i>Li Sun, Steven Versteeg, Serdar Boztaş, and Trevor Yann</i>	
Repelling Sybil-Type Attacks in Wireless Ad Hoc Systems . . . . .	391
<i>Marek Klonowski, Michał Koza, and Mirosław Kutylowski</i>	
<b>Author Index</b> . . . . .	403