Preface

The annual Australasian Conference on Information Security and Privacy (ACISP) is the premier Australian academic conference in its field, showcasing research from around the globe on a range of topics. The 16th conference in this series—ACISP 2011—was held during July 11–13, 2011, at RMIT University in Melbourne, Australia.

There were 103 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. Theoretical research features prominently in these papers.

This year the Program Committee introduced a practice of accepting some submissions for presentation as poster papers, for the first time in ACISP history. The purpose of this practice is to allow ACISP to include more practically oriented research in our program. Ten submissions were selected as poster papers. Extended abstracts for these poster papers have been included in these proceedings.

The conference program included two invited lectures by Claude Carlet of Universities of Paris 8 and 13 and CNRS, and Nick Ellsmore of Stratsec (a BAE Systems Company). Prof. Carlet spoke about “Differentially Uniform Functions” and his paper is included in the proceedings. We would like to express our gratitude to Claude and Nick for contributing their knowledge and insight, and thus expanding the horizons of the conference delegates.

We would like to thank the authors of all submissions for offering their research for presentation at ACISP 2011. We extend our sincere thanks to the Program Committee and other reviewers for the high-quality reviews and in-depth discussions. The Program Committee made use of the EasyChair electronic submission and reviewing software written by Andrei Voronkov and maintained by the University of Manchester, UK. We would like to express our thanks to Springer, particularly Alfred Hofmann, for continuing to support the ACISP conference series and for helping in the production of the conference proceedings.

We also thank the Organizing Committee, led by the ACISP 2011 General Chair Serdar Boztas, with key contributions from Leanne O’Doherty and Keith Tull, for their involvement in the conference. Finally, we would like to thank Qualcomm Incorporated, The University of Melbourne and the ISI-Informatics Research Group at RMIT University for their support, and the School of Mathematical and Geospatial Sciences at RMIT University for hosting the conference.

July 2011

Udaya Parampalli
Philip Hawkes
Organization

General Chair

Serdar Boztaş  
RMIT University, Australia

Program Co-chairs

Udaya Parampalli  
University of Melbourne, Australia
Philip Hawkes  
Qualcomm Incorporated, Australia

Program Committee

Michel Abdalla  
École Normale Supérieure, France
Magnus Almgren  
Chalmers University of Technology, Sweden
Tuomas Aura  
Microsoft Research, USA
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
Sherman Chow  
University of Waterloo, Canada
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
Christophe Doche  
Macquarie University, Australia
Pooya Farshim  
Royal Holloway, University of London, UK
Praveen Gauravaram  
Technical University of Denmark, Denmark
Peter Gutmann  
University of Auckland, New Zealand
Kwangjo Kim  
KAIST, Korea
Xuejia Lai  
Shanghai Jiao Tong University, China
Mark Manulis  
TU Darmstadt, Germany
Keith Martin  
Royal Holloway, University of London, UK
Atefeh Mashatan  
École Polytechnique Fédérale de Lausanne, Switzerland
Mitsuru Matsui  
Mitsubishi Electric, Japan
Krystian Matusiewicz  
Macquarie University, Australia
VIII Organization

Chris Mitchell
Royal Holloway, University of London, UK

Atsuko Miyaji
JAIST, Japan

Yi Mu
University of Wollongong, Australia

Rei Safavi Naini
University of Calgary, Canada

Juan Gonzalez Nieto
Queensland University of Technology, Australia

Claudio Orlandi
Aarhus University, Denmark

C. Pandu Rangan
IIT, Madras, India

Vincent Rijmen
KU Leuven, Belgium and TU Graz, Austria

Bimal Roy
Indian Statistical Institute, India

Palash Sarkar
Indian Statistical Institute, India

Jennifer Seberry
University of Wollongong, Australia

Leonie Simpson
Queensland University of Technology, Australia

Damien Stehle
École Normale Supérieure de Lyon, France

Ron Stenfield
Macquarie University, Australia

Douglas Stinson
University of Waterloo, Canada

Willy Susilo
University of Wollongong, Australia

Vijay Varadharajan
Macquarie University, Australia

Maria Isabel Gonzalez Vasco
Universidad Rey Juan Carlos, Spain

Damien Vergnaud
École Normale Supérieure, France

Huaxiong Wang
Nanyang Technological University, Singapore

Kan Yasuda
NTT, Japan

Yuliang Zheng
University of North Carolina at Charlotte, USA

External Reviewers

Ejaz Ahmed
Angelo De Caro
Erland Jonsson

Toru Akishita
Yi Deng
Kiyoto Kawauchi

Martin Albrecht
Sharmila Deva Selvi
Przemyslaw Kubiak

Kazumaro Aoki
Sun Dongdong
Yee Wei Law

Frederik Armknecht
Ming Duan
Gregor Leander

Man Ho Au
Domingo Gomez
Gaëtan Leurent

Jean-Philippe Aumasson
Zheng Gong
Allison Lewko

Manuel Barbosa
Fuchun Guo
Tingting Lin

Asli Bay
Jian Guo
Joseph Liu

Rishiraj Bhattacharyya
Jinguang Han
Zhiqiang Liu

Andrey Bogdanov
Guillaume Hanrot
Yiyuan Luo

Jens-Matthias Bohli
Islam Hegazy
Vadim Lyubashevsky

Richard Brinkman
Javier Herranz
Florian Mendel

Debrup Chakraborty
Jason Hinek
Theodosioz Mourouzis

Sanjit Chatterjee
Deukjo Hong
Sascha Müller

Kai-Yuen Cheong
Kathy Horadam
Mridul Nandi

Sherman S.M. Chow
Jinguang Huang
Kris Narayan

Cheng-Kang Chu
Xinyi Huang
Ta Toan Khoa Nguyen

Lizzie Coles-Kemp
Daniel Hulme
Abderrahmane Nitaj

Paolo D’Arco
Sebastiaan Indestege
Mehrdad Nojoumian
# Table of Contents

**Invited Talks**

On Known and New Differentially Uniform Functions ................. 1  
*Claude Carlet*

**Symmetric Key Cryptography**

New Impossible Differential Attacks of Reduced-Round Camellia-192  
and Camellia-256 ................................................................. 16  
*Jiazhe Chen, Keting Jia, Hongbo Yu, and Xiaoyun Wang*

Results on the Immunity of Boolean Functions against Probabilistic  
Algebraic Attacks ................................................................. 34  
*Meicheng Liu, Dongdai Lin, and Dingyi Pei*

Finding More Boolean Functions with Maximum Algebraic Immunity  
Based on Univariate Polynomial Representation .......................... 47  
*Yusong Du and Fangguo Zhang*

Improving the Algorithm 2 in Multidimensional Linear Cryptanalysis . . 61  
*Phuong Ha Nguyen, Hongjun Wu, and Huaxiong Wang*

State Convergence in the Initialisation of Stream Ciphers ............... 75  
*Sui-Guan Teo, Ali Al-Hamdan, Harry Bartlett, Leonie Simpson,  
Kenneth Koon-Ho Wong, and Ed Dawson*

On Maximum Differential Probability of Generalized Feistel ............ 89  
*Kazuhiko Minematsu, Tomoyasu Šuzaki, and Maki Shigeri*

Double SP-Functions: Enhanced Generalized Feistel Networks:  
Extended Abstract ........................................................................ 106  
*Andrey Bogdanov and Kyoji Shibutani*

Algebraic Techniques in Differential Cryptanalysis Revisited ............ 120  
*Meiqin Wang, Yue Sun, Nicky Mouha, and Bart Preneel*

**Hash Functions**

Faster and Smoother – VSH Revisited ........................................... 142  
*Juraj Šarínay*

Cryptanalysis of the Compression Function of SIMD .................... 157  
*Hongbo Yu and Xiaoyun Wang*
## Protocols

Electronic Cash with Anonymous User Suspension .......................... 172  
*Man Ho Au, Willy Susilo, and Yi Mu*

T-Robust Scalable Group Key Exchange Protocol with $O(\log n)$ complexity .................................................. 189  
*Tetsuya Hatano, Atsuko Miyaji, and Takashi Sato*

Application-Binding Protocol in the User Centric Smart Card Ownership Model ................................................. 208  
*Raja Naeem Akram, Konstantinos Markantonakis, and Keith Mayes*

## Access Control and Security

Security in Depth through Smart Space Cascades .......................... 226  
*Benjamin W. Long*

GeoEnc: Geometric Area Based Keys and Policies in Functional Encryption Systems .................................................. 241  
*Mingwu Zhang and Tsuyoshi Takagi*

An Efficient Rational Secret Sharing Scheme Based on the Chinese Remainder Theorem ........................................ 259  
*Yun Zhang, Christophe Tartary, and Huaxiong Wang*

DMIPS - Defensive Mechanism against IP Spoofing ......................... 276  
*Shashank Lagishetty, Pruthvi Sabbu, and Kannan Srinathan*

## Public Key Cryptography

Provably Secure Key Assignment Schemes from Factoring ............... 292  
*Eduarda S.V. Freire and Kenneth G. Paterson*

Efficient CCA-Secure CDH Based KEM Balanced between Ciphertext and Key .......................................................... 310  
*Yamin Liu, Bao Li, Xianhui Lu, and Dingding Jia*

Generic Construction of Strongly Secure Timed-Release Public-Key Encryption .................................................... 319  
*Atsushi Fujioka, Yoshiaki Okamoto, and Taiichi Saito*

Identity-Based Server-Aided Decryption ..................................... 337  
*Joseph K. Liu, Cheng Kang Chu, and Jianying Zhou*

A Generic Variant of NIST’s KAS2 Key Agreement Protocol ............. 353  
*Sanjit Chatterjee, Alfred Menezes, and Berkant Ustaoglu*
A Single Key Pair is Adequate for the Zheng Signcryption .......................... 371
Jia Fan, Yuliang Zheng, and Xiaohu Tang

Towards Public Key Encryption Scheme Supporting Equality Test with Fine-Grained Authorization .......................... 389
Qiang Tang

Posters

Lattice-Based Completely Non-malleable PKE in the Standard Model (Poster) .......................................................... 407
Reza Sepahi, Ron Steinfeld, and Josef Pieprzyk

Compliance or Security, What Cost? (Poster) .................................. 412
Craig Wright

Preimage Attacks on Full-ARIRANG (Poster) .................................. 417
Chiaki Ohtahara, Keita Okada, Yu Sasaki, and Takeshi Shimoyama

Finding Collisions for Reduced Luffa-256 v2 (Poster) .................. 423
Bart Preneel, Hirotaka Yoshida, and Dai Watanabe

Improved Security Analysis of Fugue-256 (Poster) .................. 428
Praveen Gauravaram, Lars R. Knudsen, Nasour Bagheri, and Lei Wei

Improved Meet-in-the-Middle Cryptanalysis of KTANTAN (Poster) .... 433
Lei Wei, Christian Rechberger, Jian Guo, Hongjun Wu, Huaxiong Wang, and San Ling

Toward Dynamic Attribute-Based Signcryption (Poster) .................. 439
Keita Emura, Atsuko Miyaji, and Mohammad Shahriar Rahman

A Verifiable Distributed Oblivious Transfer Protocol (Poster) ........ 444
Christian L.F. Corniaux and Hossein Ghodosi

Impracticality of Efficient PVSS in Real Life Security Standard (Poster) .......................................................... 451
Kun Peng

Electromagnetic Analysis Enhancement with Signal Processing Techniques (Poster) .......................................................... 456
Hongying Liu, Yukiyasu Tsunoo, and Satoshi Goto

Erratum

Compliance or Security, What Cost? (Poster) .................. E1
Craig Wright

Author Index .......................................................... 463