Preface

The 11th Australasian Conference on Information Security and Privacy (ACISP 2006) was held in Melbourne, 3–5 July, 2006. The conference was sponsored by Deakin University, the Research Network for a Secure Australia, and was organized in cooperation with the University of Wollongong. The conference brought together researchers, practitioners and a wide range of other users from academia, industries and government organizations.

The program included 35 papers covering important aspects of information security technologies. The papers were selected from 133 submissions through a two-stage anonymous review process. Each paper received at least three reviews by members of the Program Committee, and was then scrutinized by the whole committee during a two-week discussion. There were 19 papers eligible for the “best student paper” award. The award was given to Yang Cui from the University of Tokyo for the paper “Tag-KEM from Set Partial Domain One-Way Permutations.”

In addition to the regular papers the program also included three invited talks. Bart Preneel gave an invited talk entitled “Electronic Identity Cards: Threats and Opportunities.” Mike Burmester’s talk was “Towards Provable Security for Ubiquitous Applications.” The details of the third talk had not been finalized at the time of publication of these proceedings.

We wish to thank all the authors of submitted papers for providing the content for the conference; their high-quality submissions made the task of selecting a program very difficult. We are indebted to the diligence and enthusiasm of the Program Committee members in ensuring selection of the most deserving papers and to the external reviewers who helped in the refereeing process. We wish to thank our sponsors, Research Network for a Secure Australia, for their support of the main speakers and students as well as Springer for their continued support of ACISP. We further wish to thank Judy Chow, the conference secretary, for her many organizational skills and patience with the registration process, and our Technical Chair, Jeffrey Horton, for his continuous effort and meticulous attention to every detail, which made the task of the Program Co-chairs so much easier.

Without the help of all the above this conference would not have been a possibility.

July 2006

Lynn Batten
Reihaneh Safavi-Naini
ACISP 2006

July 3–5, 2006, Melbourne, Australia

General Chair
Lynn Batten, Deakin University, Australia

Program Co-chairs
Lynn Batten, Deakin University, Australia
Reihaneh Safavi-Naini, University of Wollongong, Australia

Technical Chair
Jeffrey Horton, University of Wollongong, Australia

Program Committee

Tuomas Aura Microsoft Research, UK
Feng Bao Institute for Infocomm Research, Singapore
Colin Boyd QUT, Australia
Liqun Chen Hewlett-Packard Laboratories, UK
Kefei Chen Shanghai Jiaotong University, China
Nicolas T. Courtois Axalto Smart Cards, France
Robert Deng Singapore Management University, Singapore
Marc Dacier Eurecom Institute, France
Ed Dawson QUT, Australia
Josep Domingo University of Tarragona, Catalonia
Dieter Gollmann Hamburg University of Technology, Germany
Juan Gonzalez Nieto QUT, Australia
Goichiro Hanaoka Nat. Inst. of Adv. Industrial Sci. and Tech., Japan
Markus Jakobsson Indiana University, USA
Marc Joye Gemplus & CIM-PACA, France
Tanja Lange Technical University of Denmark, Denmark
Byoungcheon Lee Joongbu University, Korea
Javier Lopez University of Malaga, Spain
Subhamoy Maitra Indian Statistical Institute, Kolkata, India
Catherine Meadows Naval Research Lab, USA
Atsuko Miyaji JAIST, Japan
Nasir Memon New York Polytechnic, USA
SangJae Moon Kyungpook National University, Korea
Keith Martin Royal Holloway, University of London, UK
Peng Ning North Carolina State University, USA
Kaisa Nyberg Helsinki University of Technology and Nokia, Finland
Eiji Okamoto Tsukuba University, Japan
Giuseppe Persiano Università di Salerno, Italy
Josef Pieprzyk Macquarie University, Australia
David Pointcheval CNRS/ENS, Paris, France
Bimal Roy Indian Statistical Institute, Kolkata, India
Palash Sarkar Indian Statistical Institute, India
Jennifer Seberry
University of Wollongong, Australia

Juji Shikata
Yokohama National University, Japan

Nigel Smart
University of Bristol, UK

Douglas Stinson
University of Waterloo, Canada

Tim Strayer
BBN Technologies, USA

Clark Thomborson
University of Auckland, New Zealand

Serge Vaudenay
EPFL, Switzerland

Vijay Varadharajan
Macquarie University, Australia

Victor K. Wei
Chinese University of Hong Kong, Hong Kong

External Reviewers

Masayuki Abe
Xuan Hong
Ahmed Patel

Joel Alwen
Zhenjie Huang
Kenny Paterson

Nuttapong Attrapadung
Sarat Indrakanti
Kun Peng

Robert M. Avanzi
Toshiyuki Isshiki
Pai Peng

Gildas Avoine
Tetsuya Izu
Krzysztof Pietrzak

Thomas Baignères
Christine Jones
Jordi Castellà Roca

Daniel J. Bernstein
Ari Juels
Rodrigo Roman

Srimanta Bhattacharya
Lars Knudsen
Kurt Rosenfeld

Olivier Billet
Sandeep Kumar
Chun Ruan

Mark Branagan
Noboru Kunihiro
Naouel Ben Salem

Emmanuel Bresson
Kaoru Kurosawa
Sumanta Sarkar

Jaimee Brown
Eyal Kushilevitz
Francesc Sebé

Billy Brumley
David Lapsley
Taha Sencar

Debrup Chakraborty
Jens Ove Lauf
Abdulattif Shikfa

Zhaohui Cheng
HoonJae Lee
SeongHan Shin

Andrew Clark
Corrado Leita
Leonie Simpson

Christophe Clavier
Qiming Li
Agustí Solanas

Yvonne Cliff
Ching Lin
Masakazu Soshi

Scott Contini
Joseph Liu
Ron Steinfeld

Yang Cui
Carl Livadas
Gene Tsudik

Paolo D’Arco
Yu Long
Udaya Kiran Tupakula

Vanesa Daza
Yi Lu
Ivan Visconti

Ling Dong
John Malone-Lee
Martin Vuagnoux

Ratna Dutta
Antoni Martín-Ballesté
Zhiguo Wan

Stefan Dziembowski
Sebastia Martin
Guilin Wang

Sarah Edwards
Krystian Matusiewicz
Huaxiong Wang

Mari Carmen Fernandez-Gago
Bill Millan
Pan Wang

Matthieu Finiasz
Hideyuki Miyake
Ruizhong Wei

Eiichiro Fujisaki
Kunihiko Miyazaki
Mi Wen

Jun Furukawa
Jean Monnerat
Jian Weng

Clemente Galdi
Mridul Nandy
Christopher Wolf

Zheng Gong
Stan Nulislov
Katsunari Yoshioka

Aline Gouget
Wakaha Ogata
Qinghua Zhang

Vanessa Gratzer
Juan J. Ortega
Rui Zhang

Jens Groth
Akira Otsuka
Weiliang Zhao

Jaechol Ha
Vikram PAdman
Huafei Zhu

Matt Henricksen
Dan Page

Jason Hinek
Sylvain Pasini
# Table of Contents

## Stream Ciphers

Algebraic Attacks on Clock-Controlled Stream Ciphers  
*Sultan Al-Hinai, Lynn Batten, Bernard Colbert, Kenneth Wong*  
.......................................................... 1

Cache Based Power Analysis Attacks on AES  
*Jacques Fournier, Michael Tunstall*  
......................................................... 17

Distinguishing Attack on SOBER-128 with Linear Masking  
*Joo Yeon Cho, Josef Pieprzyk*  
.......................................................... 29

Evaluating the Resistance of Stream Ciphers with Linear Feedback Against Fast Algebraic Attacks  
*An Braeken, Joseph Lano, Bart Preneel*  
......................................................... 40

## Symmetric Key Ciphers

Ensuring Fast Implementations of Symmetric Ciphers on the Intel Pentium 4 and Beyond  
*Matt Henricksen, Ed Dawson*  
.......................................................... 52

Improved Cryptanalysis of MAG  
*Leonie Simpson, Matt Henricksen*  
.......................................................... 64

On Exact Algebraic [Non-]Immunity of S-Boxes Based on Power Functions  
*Nicolas T. Courtois, Blandine Debraize, Eric Garrido*  
.......................................................... 76

## Network Security

Augmented Certificate Revocation Lists  
*A. Lakshminarayanan, T.L. Lim*  
.......................................................... 87

Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security  
*Shidi Xu, Yi Mu, Willy Susilo*  
.......................................................... 99

Towards an Invisible Honeypot Monitoring System  
*Nguyen Anh Quynh, Yoshiyasu Takefuji*  
.......................................................... 111
Cryptographic Applications

Adaptively Secure Traitor Tracing Against Key Exposure and Its Application to Anywhere TV Service
Kazuto Ogawa, Goichiro Hanaoka, Hideki Imai ........................................ 123

Fingercasting—Joint Fingerprinting and Decryption of Broadcast Messages
André Adelsbach, Ulrich Huber, Ahmad-Reza Sadeghi ....................... 136

More on Stand-Alone and Setup-Free Verifiably Committed Signatures
Huafei Zhu, Feng Bao ............................................. 148

Secure Implementation

API Monitoring System for Defeating Worms and Exploits in MS-Windows System
Hung-Min Sun, Yue-Hsun Lin, Ming-Fung Wu .......................... 159

Hiding Circuit Topology from Unbounded Reverse Engineers
Yu Yu, Jussipekka Leiwo, Benjamin Premkumar ......................... 171

The Role of the Self-Defending Object Concept in Developing Distributed Security-Aware Applications
John W. Holford, William J. Caelli ...................................... 183

Signatures

Efficient and Provably Secure Multi-receiver Identity-Based Signcryption
Shanshan Duan, Zhenfu Cao ............................................. 195

Efficient Identity-Based Signatures Secure in the Standard Model
Kenneth G. Paterson, Jacob C.N. Schuldt .................................. 207

Event-Oriented $k$-Times Revocable-iff-Linked Group Signatures
Man Ho Au, Willy Susilo, Siu-Ming Yiu ....................... 223

Key Replacement Attack Against a Generic Construction of Certificateless Signature
Bessie C. Hu, Duncan S. Wong, Zhenfeng Zhang, Xiaotie Deng ................. 235
Theory

A Novel Range Test
Kun Peng, Colin Boyd, Ed Dawson, Eiji Okamoto .......................... 247

Efficient Primitives from Exponentiation in $\mathbb{Z}_p$
Shaoquan Jiang ............................................................... 259

PA in the Two-Key Setting and a Generic Conversion for Encryption with Anonymity
Ryotaro Hayashi, Keisuke Tanaka ........................................ 271

Statistical Decoding Revisited
R. Overbeck ........................................................................ 283

Invited Talk

Towards Provable Security for Ubiquitous Applications
Mike Burmester, Tri Van Le, Breno de Medeiros ...................... 295

Security Applications

Oblivious Scalar-Product Protocols
Huafei Zhu, Feng Bao ......................................................... 313

On Optimizing the $k$-Ward Micro-aggregation Technique for Secure Statistical Databases
Ebaa Fayyoumi, B. John Oommen ........................................ 324

Provable Security

Direct Chosen-Ciphertext Secure Identity-Based Key Encapsulation Without Random Oracles
Eike Kiltz, David Galindo .................................................... 336

Generic Transforms to Acquire CCA-Security for Identity Based Encryption: The Cases of FOPKC and REACT
Takashi Kitagawa, Peng Yang, Goichiro Hanaoka, Rui Zhang,
Hajime Watanabe, Kanta Matsuura, Hideki Imai ........................ 348

Tag-KEM from Set Partial Domain One-Way Permutations
Masayuki Abe, Yang Cui, Hideki Imai, Kaoru Kurosawa ............. 360
Protocols

An Extension to Bellare and Rogaway (1993) Model: Resetting Compromised Long-Term Keys
   Colin Boyd, Kim-Kwang Raymond Choo, Anish Mathuria ........................ 371

Graphical Representation of Authorization Policies for Weighted Credentials
   Isaac Agudo, Javier Lopez, Jose A. Montenegro ................................. 383

Secure Cross-Realm C2C-PAKE Protocol
   Yin Yin, Li Bao ................................................................. 395

Hashing and Message Authentication

Constructing Secure Hash Functions by Enhancing Merkle-Damgård Construction
   Praveen Gauravaram, William Millan, Ed Dawson, Kapali Viswanathan .... 407

Forgery and Key Recovery Attacks on PMAC and Mitchell’s TMAC Variant
   Changhoon Lee, Jongsung Kim, Jaechul Sung, Seokhie Hong, Sangjin Lee 421

Side Channel Attacks Against HMACs Based on Block-Cipher Based Hash Functions
   Katsuyuki Okeya ............................................................... 432

Author Index ................................................................. 445