

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

Alfred Kobsa

University of California, Irvine, CA, 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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Willy Susilo Yi Mu Jennifer Seberry (Eds.)

Information Security and Privacy

17th Australasian Conference, ACISP 2012
Wollongong, NSW, Australia, July 9-11, 2012
Proceedings

Volume Editors

Willy Susilo

Yi Mu

Jennifer Seberry

University of Wollongong

School of Computer Science and Software Engineering

Northfields Avenue

Wollongong, NSW 2522, Australia

E-mail: {wsusilo; ymu; jennie}@uow.edu.au

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-31447-6

e-ISBN 978-3-642-31448-3

DOI 10.1007/978-3-642-31448-3

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012940392

CR Subject Classification (1998): K.6.5, E.3, D.4.6, E.4, J.1, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 17th Australasian Conference on Information Security and Privacy (ACISP 2012) was held at Wollongong, Australia, during July 9–11, 2012. The conference was sponsored by the Centre for Computer and Information Security of the University of Wollongong. The submission and review process was run using the iChair software, written by Thomas Baigneres and Matthieu Finiasz from EPFL, LASEC, Switzerland. We would like to thank them for letting us use their iChair software.

The conference received 89 submissions, out of which the Program Committee selected 30 full papers and 5 short papers for presentation at the conference after a rigorous review process. These papers are included in the proceedings. The accepted papers cover a range of topics in information security, including some fundamental theory, cryptanalysis, message authentications, hash functions, public key cryptography, digital signatures, identity-based cryptography, attribute-based cryptography, lattice-based cryptography, lightweight cryptography and RFIDs. The conference proceedings contain revised versions of the selected papers. Since some of them were not checked again for correctness before publication, the authors bear full responsibility for the contents of their papers. We would like to thank the authors of all papers for submitting their work to the conference.

In addition to the contributed papers, the program included two invited talks. The invited speakers were Mihir Bellare (University of California, San Diego), with the topic “A Cryptographic Treatment of the Wiretap Channel” and Jorge Munilla (Universidad de Málaga, Spain), with the topic “Operating Principles of RFID Systems and Attacks Related to the Location.” We would like to express our thanks to them.

As in previous years, we selected a “best student paper.” To be eligible for selection, a paper has to be co-authored by a postgraduate student, whose contribution was more than 50%. The winner was Xuhua Zhou from Shanghai Jiao Tong University, P.R. China, for the paper “A Generic Construction of Accountable Decryption and Its Applications.”

We would like to thank all the people who helped with the conference program and organization. In particular, we heartily thank the Program Committee and the sub-reviewers listed on the following pages for the effort and time they contributed to the review process. A special thanks to the Publication Chair, Man Ho Au, who spent a tremendous amount of time for the success of the conference. We would also like to express our thanks to Springer for continuing to support the ACISP conference and for help in the conference proceedings production.

Finally, we would like to thank the General Chair, Jennifer Seberry, and the Organizing Committee for their excellent contribution to the conference.

July 2012

Willy Susilo
Yi Mu

Organization

General Chair

Jennifer Seberry University of Wollongong, Australia

Program Chairs

Willy Susilo University of Wollongong, Australia

Yi Mu University of Wollongong, Australia

Program Committee

Michel Abdalla	École Normale Supérieure, France
Joonsang Baek	Khalifa University, United Arab Emirates
Alex Biryukov	Université du Luxembourg, Luxembourg
Paulo Barreto	University of São Paulo, Brazil
Feng Bao	Institute for Infocomm Research, Singapore
Lynn Batten	Deakin University, Australia
Colin Boyd	Queensland University of Technology, Australia
Serdar Boztas	RMIT, Australia
Xiaofeng Chen	Xidian University, China
Nicolas T. Courtois	University College London, UK
Yvo Desmedt	University College London, UK
Orr Dunkelman	University of Haifa, Israel
Steven Galbraith	University of Auckland, New Zealand
Qiong Huang	South China Agricultural University, PR China
Xinyi Huang	Fujian Normal University, PR China
Apu Kapadia	Indiana University Bloomington, USA
Xuejia Lai	Shanghai Jiaotong University, China
Dong Hoon Lee	Electronics and Telecommunications Research Institute, Korea
Keith Martin	Royal Holloway, University of London, UK
Chris Mitchell	Royal Holloway, University of London, UK
Fabien Laguilaumie	UCBN and CNRS, LIP (Lyon), France
Atsuko Miyaji	Japan Advanced Institute of Science and Technology, Japan
Juan Gonzales Nieto	Queensland University of Technology, Australia
Miyako Ohkubo	National Institute of Information and Communications Technology, Japan
Claudio Orlandi	Bar-Ilan University, Israel
Udaya Parampalli	University of Melbourne, Australia

VIII Organization

Josef Pieprzyk	Macquarie University, Australia
Mark Ryan	University of Birmingham, UK
Rei Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Ron Steinfeld	Macquarie University, Australia
Douglas Stinson	University of Waterloo, Canada
Tsuyoshi Takagi	Kyushu University, Japan
Vijay Varadharajan	Macquarie University, Australia
Kan Yasuda	NTT Corporation, Japan
Guilin Wang	University of Wollongong, Australia
Huaxiong Wang	Nanyang Technological University, Singapore
Duncan S. Wong	City University of Hong Kong, Hong Kong
Shouhuai Xu	University of Texas at San Antonio, USA
Guomin Yang	National University of Singapore, Singapore

Publication Chair

Man Ho Au	University of Wollongong, Australia
-----------	-------------------------------------

Organizing Committee

Fuchun Guo	University of Wollongong, Australia
Thomas Plantard	University of Wollongong, Australia
Reza Reyhanitabar	University of Wollongong, Australia

External Reviewers

Manal Adham	Matt Henricksen	Fagen Li
Yoshinori Aono	Javier Herranz	Jin Li
Myrto Arapinis	Mathias Herrmann	Shen Li
Gilad Asharov	Qiong Huang	Tieyan Li
Sergiu Bursuc	Hyoseung Kim	Kaitai Liang
Guilhem Castagnos	Kitak Kim	Hoon Wei Lim
Melissa Chase	Milyoung Kim	Richard Lindner
Yuan Chen	Aleksandar Kircanski	Zhen Liu
Kai-Yuen Cheong	Woo Kwon Koo	Jiqiang Lu
Koji Chida	Ozgul Kucuk	Weiliang Luo
Bernard Colbert	Lakshmi Kuppusamy	Shah Mahmood
Anupam Datta	Junzuo Lai	Cuauhtemoc
Angelo De Caro	Yee Wei Law	Mancillas-Lopez
Wei Gao	Hoi Le	Pedro Maat Massolino
Jian Guo	Kwangsue Lee	Seiichi Matsuda
Guillaume Hanrot	Peter Lee	Kirill Morozov
Takuya Hayashi	Gaëtan Leurent	Shishir Nagaraja

Prasad G. Naldurg
Ta Toan Khoa Nguyen
Shirin Nilizadeh
Ryo Nishimaki
Kazumasa Omote
Jong Hwan Park
Seunghwan Park
Geovandro Pereira
Duong Hieu Phan
Haifeng Qian
Hasan Qunoo
Kenneth Radke
Somindu C. Ramanna
Asha Rao
Arnab Roy
Moustafa Saleh

Sumanta Sarkar
Yu Sasaki
Roman Schlegel
Jae Hong Seo
Naoyuki Shinohara
Leonie Simpson
Dondong Sun
Li Sun
Katsuyuki Takashima
Xiao Tan
Keisuke Tanaka
Fei Tang
Ashraful Tuhin
Fenghe Wang
Lihua Wang
Yongzhuang Wei

Li Xu
Piyi Yang
Yanjiang Yang
Masaya Yasuda
Bin Zhang
Hui Zhang
Kehuan Zhang
Liangfeng Zhang
Mingwu Zhang
Rui Zhang
Yinghui Zhang
Yun Zhang
Qingji Zheng
Huafei Zhu
Youwen Zhu

Table of Contents

Fundamentals

Optimal Bounds for Multi-Prime Φ -Hiding Assumption	1
<i>Kaori Tosu and Noboru Kunihiro</i>	
Sufficient Condition for Ephemeral Key-Leakage Resilient Tripartite Key Exchange	15
<i>Atsushi Fujioka, Mark Manulis, Koutarou Suzuki, and Berkant Ustaoglu</i>	
A Game-Theoretic Perspective on Oblivious Transfer	29
<i>Haruna Higo, Keisuke Tanaka, Akihiro Yamada, and Kenji Yasunaga</i>	
Faster Algorithm for Solving Hard Knapsacks for Moderate Message Length	43
<i>Yuji Nagashima and Noboru Kunihiro</i>	
Accelerating the Secure Distributed Computation of the Mean by a Chebyshev Expansion	57
<i>Peter Lory and Manuel Liedel</i>	

Cryptanalysis

Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo	71
<i>Takanori Isobe and Kyoji Shibutani</i>	
Improved Known-Key Distinguishers on Feistel-SP Ciphers and Application to Camellia	87
<i>Yu Sasaki, Sareh Emami, Deukjo Hong, and Ashish Kumar</i>	
Low Data Complexity Attack on Reduced Camellia-256	101
<i>Jiazhe Chen and Leibo Li</i>	
Cryptanalysis of RSA with a Small Parameter	115
<i>Xianmeng Meng and Xuexin Zheng</i>	
An Algebraic Broadcast Attack against NTRU	124
<i>Jintai Ding, Yanbin Pan, and Yingpu Deng</i>	

Message Authentication Codes and Hash Functions

Analysis of Indirect Message Injection for MAC Generation Using Stream Ciphers	138
<i>Mufeed ALMashrafi, Harry Bartlett, Leonie Simpson, Ed Dawson, and Kenneth Koon-Ho Wong</i>	

WEIMAR-DM: A Highly Secure Double-Length Compression Function	152
<i>Ewan Fleischmann, Christian Forler, Stefan Lucks, and Jakob Wenzel</i>	

Public Key Cryptography

An Efficient IND-CCA2 Secure Variant of the Niederreiter Encryption Scheme in the Standard Model	166
<i>Preetha Mathew K., Sachin Vasant, Sridhar Venkatesan, and C. Pandu Rangan</i>	

Zero-Knowledge Protocols for the McEliece Encryption	180
<i>Kirill Morozov and Tsuyoshi Takagi</i>	

Effort-Release Public-Key Encryption from Cryptographic Puzzles	194
<i>Jothi Rangasamy, Douglas Stebila, Colin Boyd, Juan Manuel González-Nieto, and Lakshmi Kuppasamy</i>	

Leakage-Resilience of Stateless/Stateful Public-Key Encryption from Hash Proofs	208
<i>Manh Ha Nguyen, Keisuke Tanaka, and Kenji Yasunaga</i>	

How to Fix Two RSA-Based PVSS Schemes—Exploration and Solution	223
<i>Kun Peng and Matt Henricksen</i>	

Digital Signatures

Relation between Verifiable Random Functions and Convertible Undeniable Signatures, and New Constructions	235
<i>Kaoru Kurosawa, Ryo Nojima, and Le Trieu Phong</i>	

Generalized First Pre-image Tractable Random Oracle Model and Signature Schemes	247
<i>Xiao Tan and Duncan S. Wong</i>	

A Short Non-delegatable Strong Designated Verifier Signature	261
<i>Haibo Tian, Xiaofeng Chen, and Jin Li</i>	
Deterministic Identity Based Signature Scheme and Its Application for Aggregate Signatures	280
<i>S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan</i>	
Fully Leakage-Resilient Signatures with Auxiliary Inputs	294
<i>Tsz Hon Yuen, Siu Ming Yiu, and Lucas C.K. Hui</i>	

Identity-Based and Attribute-Based Cryptography

Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts	308
<i>Duong-Hieu Phan, David Pointcheval, Siamak F. Shahandashti, and Mario Strefler</i>	
A Generic Construction of Accountable Decryption and Its Applications	322
<i>Xuhua Zhou, Xuhua Ding, and KeFei Chen</i>	
Threshold Ciphertext Policy Attribute-Based Encryption with Constant Size Ciphertexts	336
<i>Aijun Ge, Rui Zhang, Cheng Chen, Chuanguai Ma, and Zhenfeng Zhang</i>	
Fully Private Revocable Predicate Encryption	350
<i>Juan Manuel González-Nieto, Mark Manulis, and Dongdong Sun</i>	
Anonymous ID-Based Proxy Re-Encryption	364
<i>Jun Shao</i>	

Lattice-Based Cryptography

On the Optimality of Lattices for the Coppersmith Technique	376
<i>Yoshinori Aono, Manindra Agrawal, Takakazu Satoh, and Osamu Watanabe</i>	
Revocable Identity-Based Encryption from Lattices	390
<i>Jie Chen, Hoon Wei Lim, San Ling, Huaxiong Wang, and Khoa Nguyen</i>	

Lightweight Cryptography

On Area, Time, and the Right Trade-Off	404
<i>A. Poschmann and M.J.B. Robshaw</i>	

Short Papers

Analysis of Xorrotation with Application to an HC-128 Variant	419
<i>Paul Stankovski, Martin Hell, and Thomas Johansson</i>	
Private Fingerprint Matching	426
<i>Siamak F. Shahandashti, Reihaneh Safavi-Naini, and Philip Ogunbona</i>	
Minimizing Information Leakage of Tree-Based RFID Authentication Protocols Using Alternate Tree-Walking	434
<i>Kaleb Lee, Colin Boyd, and Juan Manuel González-Nieto</i>	
ICAF: A Context-Aware Framework for Access Control	442
<i>A.S.M. Kayes, Jun Han, and Alan Colman</i>	
Non-malleable Instance-Dependent Commitment in the Standard Model	450
<i>Wenpan Jing, Hairia Xu, and Bao Li</i>	
Author Index	459