More information about this series at http://www.springer.com/series/7410
Preface

This volume contains the papers presented at ACISP 2015: the 20th Australasian Conference on Information Security and Privacy held from June 29 to July 1, 2015, in Brisbane, Australia. The conference was hosted by the Institute for Future Environments at the Queensland University of Technology, who provided the wonderful facilities and material support. The local Organizing Committee was led by the ACISP 2015 general chair, Josef Pieprzyk, with administration led by Cindy Mayes. We appreciate the support of Ed Dawson and Seyit Camtepe in the conference organization. We made use of the excellent EasyChair submission and reviewing software.

There were 112 submissions. Each submission was allocated to three Program Committee members and each paper received on average 2.9 reviews. The committee decided to accept 28 papers. Accepted papers came from 13 countries with the largest proportions coming from Australia (6), Japan (6), India (5), China (4), and Germany (2). Other authors are from Belgium, Canada, France, Luxembourg, The Netherlands, New Zealand, Singapore, and the USA. We would like to extend our sincere thanks to all authors who submitted papers to ACISP 2015.

The program also included three excellent and informative invited talks. One of these was from an eminent cryptography researcher and the other two were from highly experienced security practitioners: Professor Colin Boyd, from the Norwegian University of Science and Technology (NTNU); Jason Smith, from CERT Australia; and Simon Pope, from the Microsoft Security Response Center.

We would like to thank the team of experts who made up the Program Committee. Their names are listed overleaf. The Program Committee was assisted by an even larger team of people who reviewed papers in their area of expertise. The list of these reviewers is also included. Finally, we would like to thank Springer for their help with the production of these conference proceedings and their commitment to the ACISP conference for the last 20 years. We look forward to many more years of ACISP.

June 2015

Ernest Foo
Douglas Stebila
Organization

Program Committee

Joonsang Baek  
Khalifa University of Science, Technology and Research, UAE
Paulo Barreto  
University of São Paulo, Brazil
Alex Biryukov  
University of Luxembourg, Luxembourg
Colin Boyd  
Norwegian University of Science and Technology (NTNU), Norway
Xavier Boyen  
Queensland University of Technology, Australia
Jean Camp  
Indiana University, USA
Kim-Kwang Raymond Choo  
University of South Australia, Australia
K.P. Chow  
University of Hong Kong, SAR China
Craig Costello  
Microsoft Research
Cas Cremers  
University of Oxford, UK
Marc Fischlin  
Technical University of Darmstadt, Germany
Ernest Foo  
Queensland University of Technology, Australia
Praveen Gauravaram  
Queensland University of Technology, Australia
Joanne L. Hall  
Queensland University of Technology, Australia
Jiankun Hu  
University of New South Wales at ADFA, Australia
Tancrède Lepoint  
CryptoExperts
Sachin Lodha  
Tata Consultancy Services
Mark Manulis  
University of Surrey, UK
Atsuko Miyaji  
Japan Advanced Institute of Science and Technology, Japan
Yi Mu  
University of Wollongong, Australia
C. Pandu Rangan  
Indian Institute of Technology, Madras, India
Udaya Parampalli  
University of Melbourne, Australia
Rei Safavi-Naini  
University of Calgary, Canada
Palash Sarkar  
Indian Statistical Institute, India
Jennifer Seberry  
University of Wollongong, Australia
Leonie Simpson  
Queensland University of Technology, Australia
Douglas Stebila  
Queensland University of Technology, Australia
Suriadi Suriadi  
Massey University, New Zealand
Willy Susilo  
University of Wollongong, Australia
Tsuyoshi Takagi  
Kyushu University, Japan
Berkant Ustaoglu  
NTT Information Sharing Platform Laboratories
Vijay Varadharajan  
Macquarie University, Australia
Kan Yasuda  
NTT Secure Platform Laboratories
Jianying Zhou  
Institute for Infocomm Research, Singapore
Additional Reviewers

Abdelraheem, Mohamed Ahmed
Aditya, Riza
Alkhzaimi, Hoda
Aoki, Kazumaro
Bagheri, Nasour
Baignères, Thomas
Bouzefrane, Samia
Bringer, Julien
Chalamala, Srinivas
Chen, Jiageng
Cheng, Shu
D’Orazio, Christian
Damavandinejadmonfared, Sepehr
Dawson, Ed
Delerablé, Cécile
Derbez, Patrick
Devash, Sharmila
Dilruba, Raushan
Dong, Xinshu
Dong, Zheng
Dowling, Benjamin
Dunkelman, Orr
Emmadi, Nitesh
Fan, Jia
Fehr, Victoria
Futa, Yuichi
Gagliardoni, Tommaso
Garratt, Luke
Guo, Fuchun
Han, Jinguang
Henriksen, Matt
Hitchens, Michael
Hou, Shuhui
Huang, Kun
Huang, Qiong
Jhawar, Mahavir Jhawar
Jindal, Arun
Kamara, Seny
Karande, Shirish
Khovratovich, Dmitri
Kojima, Tetsuya
Kumari, Rashmi
Laarhoven, Thijs
Liang, Kaitai
Lin, Fuchun
Liu, Joseph
Liu, Zhenhua
Longa, Patrick
Lopez-Alt, Adriana
Luykx, Atul
Manjunath, R. Sumesh
Marson, Giorgia Azzurra
Min, Byungho
Mittelbach, Arno
Mouha, Nick
Naehrig, Michael
Narumanchi, Harika
Neves, Samuel
Nikova, Svetla
Ohtake, Go
Omote, Kazumasa
Perrin, Léo Paul
Poettering, Bertram
Pustogarov, Ivan
Radke, Kenneth
Roy, Sujoy Sinha
Sadeghian, Saeed
Sasaki, Yu
Shull, Adam
Similicio Jr, Marcos
Soltan Panah, Arezou
Su, Chunhua
Syed, Habeeb
Tanaka, Satoru
Teske-Wilson, Edlyn
Todo, Yosuke
Tupakula, Uday
Tupsamudre, Harshal
Udovenko, Aleksei
Velichkov, Vesselin
Wang, Pengwei
Wu, Wei
Xu, Jia
Xu, Rui
Yang, Guomin
Yasuda, Masaya
Yasuda, Takanori
Zhang, Hui
Zhang, Mingwu
Zhou, Lan
Contents

Symmetric Cryptanalysis

Weak-Key and Related-Key Analysis of Hash-Counter-Hash Tweakable Enciphering Schemes .................................................. 3
Zhelei Sun, Peng Wang, and Liting Zhang

Cryptanalysis of Reduced-Round Whirlwind .......................... 20
Bingke Ma, Bao Li, Ronglin Hao, and Xiaqian Li

Improving the Biclique Cryptanalysis of AES ....................... 39
Biaoshuai Tao and Hongjun Wu

Public Key Cryptography

A New General Framework for Secure Public Key Encryption with Keyword Search ......................................................... 59
Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo, and Xiaofen Wang

Dynamic Threshold Public-Key Encryption with Decryption Consistency from Static Assumptions ............................... 77
Yusuke Sakai, Keita Emura, Jacob C.N. Schuldt, Goichiro Hanaoka, and Kazuo Ohta

Sponge Based CCA2 Secure Asymmetric Encryption for Arbitrary Length Message ....................................................... 93
Tarun Kumar Bansal, Donghoon Chang, and Somitra Kumar Sanadhya

Trade-Off Approaches for Leak Resistant Modular Arithmetic in RNS ...... 107
Christophe Negre and Guilherme Perin

Identity-Based Encryption

Towards Forward Security Properties for PEKS and IBE. .......... 127
Qiang Tang

IBE Under k-LIN with Shorter Ciphertexts and Private Keys ........ 145
Kaoru Kurosawa and Le Trieu Phong

Improved Identity-Based Online/Offline Encryption ................. 160
Jianchang Lai, Yi Mu, Fuchun Guo, and Willy Susilo
Constructions of CCA-Secure Revocable Identity-Based Encryption
Yuu Ishida, Yohei Watanabe, and Junji Shikata

Digital Signatures

Linkable Message Tagging: Solving the Key Distribution Problem of Signature Schemes
Felix Günther and Bertram Poettering

Generic Transformation to Strongly Existentially Unforgeable Signature Schemes with Continuous Leakage Resiliency
Yuyu Wang and Keisuke Tanaka

Constant Size Ring Signature Without Random Oracle
Priyanka Bose, Dipanjan Das, and Chandrasekharan Pandu Rangan

Security Protocols

Constant-Round Leakage-Resilient Zero-Knowledge Argument for NP from the Knowledge-of-Exponent Assumption
Tingting Zhang, Hongda Li, and Guifang Huang

Modelling Ciphersuite and Version Negotiation in the TLS Protocol
Benjamin Dowling and Douglas Stebila

VisRAID: Visualizing Remote Access for Intrusion Detection
Leliel Trethowen, Craig Anslow, Stuart Marshall, and Ian Welch

BP-XACML an Authorisation Policy Language for Business Processes
Khalid Alissa, Jason Reid, Ed Dawson, and Farzad Salim

Symmetric Cryptanalysis

How TKIP Induces Biases of Internal States of Generic RC4
Ryoma Ito and Atsuko Miyaji

Preventing Fault Attacks Using Fault Randomization with a Case Study on AES
Shamit Ghosh, Dhiman Saha, Abhrajit Sengupta, and Dipanwita Roy Chowdhury

Analysis of Rainbow Tables with Fingerprints
Gildas Avoine, Adrien Bourgeois, and Xavier Carpent
### Privacy Protocols

A New Public Remote Integrity Checking Scheme with User Privacy

*Yiteng Feng, Yi Mu, Guomin Yang, and Joseph K. Liu*

Efficient Dynamic Provable Data Possession with Public Verifiability and Data Privacy

*Clémentine Gritti, Willy Susilo, and Thomas Plantard*

Privately Computing Set-Union and Set-Intersection Cardinality via Bloom Filters

*Rolf Egert, Marc Fischlin, David Gens, Sven Jacob, Matthias Senker, and Jörn Tillmanns*

### Symmetric Constructions

Generalizing PMAC Under Weaker Assumptions

*Nilanjan Datta and Kan Yasuda*

sp-AELM: Sponge Based Authenticated Encryption Scheme for Memory Constrained Devices

*Megha Agrawal, Donghoon Chang, and Somitra Sanadhya*

### Homomorphic Encryption and Obfuscation

Secure Statistical Analysis Using RLWE-Based Homomorphic Encryption

*Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, and Takeshi Koshiba*

Bad Directions in Cryptographic Hash Functions

*Daniel J. Bernstein, Andreas Hülsing, Tanja Lange, and Ruben Niederhagen*

### Author Index

*509*