

Lecture Notes in Computer Science

13915

Founding Editors


Gerhard Goos


Juris Hartmanis

Editorial Board Members

Elisa Bertino, *Purdue University, West Lafayette, IN, USA*

Wen Gao, *Peking University, Beijing, China*

Bernhard Steffen , *TU Dortmund University, Dortmund, Germany*

Moti Yung , *Columbia University, New York, NY, USA*

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.


Leonie Simpson · Mir Ali Rezazadeh Bae
Editors

Information Security and Privacy

28th Australasian Conference, ACISP 2023
Brisbane, QLD, Australia, July 5–7, 2023
Proceedings

Editors

Leonie Simpson 
Queensland University of Technology
Brisbane, QLD, Australia

Mir Ali Rezazadeh Baei 
Queensland University of Technology
Brisbane, QLD, Australia

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-35485-4

ISBN 978-3-031-35486-1 (eBook)

<https://doi.org/10.1007/978-3-031-35486-1>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2023

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the refereed papers presented at the 28th Australasian Conference on Information Security and Privacy (ACISP 2023). The conference was held on 5–7 July 2023, in Brisbane, Australia and hosted by Queensland University of Technology, who provided excellent facilities and support.

The ACISP conference has been an annual event since 1996, and brings together security researchers and practitioners from academia, industry and government organizations for presentation of current developments and challenges in the domain of information security and privacy. After several years of virtual and hybrid conferences due to the COVID pandemic restrictions, 2023 marked a return to a physical conference, with opportunities to network and socialize in addition to the formal program of presentations.

For ACISP 2023, we made use of the EasyChair submission and reviewing software. The Program Committee selected 27 research papers from the 87 submissions received, following a double-blind reviewing process. Each submission received at least three reviews, and the reviewer feedback was provided to all submitting authors. We thank all authors of submitted papers - the high quality of the submissions made the task of selecting a program difficult.

This volume contains the revised versions of the 27 accepted papers. We express our thanks to Springer for their continued support of ACISP, and for their help with the conference proceedings production.

We are grateful for the efforts of the Program Committee members and external reviewers, who applied their knowledge and expertise in reviewing submissions, participating in discussions to determine which papers would be selected and providing feedback to the authors. Our deepest thanks for your efforts. The ACISP-2023 Program Committee represents both geographic and gender diversity: members were from 18 nations, and almost 35% of the committee were female. We hope future ACISP committees will continue to progress towards gender equality.

In addition to the selected research papers, the ACISP-2023 program included four invited talks on aspects of information security and privacy practice and research. QUT's Vice President (Administration) and Registrar, Leanne Harvey, spoke on the December 2022 cyber-attack on QUT. The Cyber Security CRC Research Director, Helge Janicke, discussed security research collaboration between academia, government and industry. The historical development of communications security capabilities in government was outlined, and Lennon Chang (Deakin University) talked about cultural aspects of privacy. Details of their presentations do not appear in these proceedings. However, we thank all these speakers for sharing their insight and inspiring continuing research in the information security and privacy domains.

We acknowledge the contribution of our local organizing committee members: QUT staff and research students in the Information Security discipline, whose efforts enabled the smooth running of the conference. We make special mention of a former longstanding

QUT staff member, Ed Dawson. Ed had a long involvement with ACISP, and was involved in the planning for ACISP 2023. Sadly, he passed away earlier this year. He will be greatly missed.

July 2023

Leonie Simpson
Mir Ali Rezazadeh Bae

Organization

General Chair

Josef Pieprzyk

Commonwealth Scientific and Industrial Research
Organization, Data61, Australia

Publication Chairs

Leonie Simpson

Queensland University of Technology, Australia

Mir Ali Rezazadeh Bae

Queensland University of Technology, Australia

Program Committee Chairs

Leonie Simpson

Queensland University of Technology, Australia

Mir Ali Rezazadeh Bae

Queensland University of Technology, Australia

Program Committee Members

Cristina Alcaraz

University of Malaga, Spain

Elena Andreeva

Technische Universität Wien, Austria

Man Ho Au

University of Hong Kong, Hong Kong

Shi Bai

Florida Atlantic University, USA

Harry Bartlett

Queensland University of Technology, Australia

Lejla Batina

Radboud University, The Netherlands

Rishiraj Bhattacharyya

University of Birmingham, UK

Colin Boyd

Norwegian University of Science and Technology,
Norway

Rongmao Chen

National University of Defense Technology,
China

Chitchanok Chuengsatiansup

University of Melbourne, Australia

Amy Corman

RMIT University, Australia

Craig Costello

Microsoft Research, USA

Hui Cui

Murdoch University, Australia

Edward Dawson

Queensland University of Technology, Australia

Josep Domingo-Ferrer

Universitat Rovira i Virgili, Spain

Rafael Dowsley	Monash University, Australia
Keita Emura	National Institute of Information and Communications Technology, Japan
Ernest Foo	Griffith University, Australia
Debin Gao	Singapore Management University, Singapore
Joanne Hall	RMIT University, Australia
Jinguang Han	Southeast University, China
Jingnan He	Institute of Information Engineering of Chinese Academy of Sciences, China
Swee-Huay Heng	Multimedia University, Malaysia
Xiaolu Hou	Slovak University of Technology, Slovakia
Qiong Huang	South China Agricultural University, China
Malika Izabachène	Cosmian, France
Zahra Jadidi	Griffith University, Australia
Angelos Keromytis	Georgia Institute of Technology, USA
Dan Kim	University of Queensland, Australia
Veronika Kuchta	Florida Atlantic University, USA
Fabien Laguillaumie	University of Montpellier, LIRMM, France
Hyung Tae Lee	Chung-Ang University, South Korea
Yannan Li	University of Wollongong, Australia
Yingjiu Li	University of Oregon, USA
Shengli Liu	Shanghai Jiao Tong University, China
Yuhong Liu	Santa Clara University, USA
Rongxing Lu	University of New Brunswick, Canada
Xianhui Lu	Institute of Information Engineering, CAS, China
Siqi Ma	University of New South Wales, Australia
Mitsuru Matsui	Mitsubishi Electric, Japan
Matthew McKague	Queensland University of Technology, Australia
Weizhi Meng	Technical University of Denmark, Denmark
Chris Mitchell	Royal Holloway, University of London, UK
Kirill Morozov	University of North Texas, USA
Khoa Nguyen	University of Wollongong, Australia
Lei Pan	Deakin University, Australia
Dimitrios Papadopoulos	Hong Kong University of Science and Technology, Hong Kong
Udaya Parampalli	University of Melbourne, Australia
Josef Pieprzyk	CSIRO/Data61, Australia
Indrakshi Ray	Colorado State University, USA
Adeline Roux-Langlois	CNRS, IRISA, France
Reihaneh Safavi-Naini	University of Calgary, Canada
Amin Sakzad	Monash University, Australia
Pierangela Samarati	Università degli Studi di Milano, Italy

Luisa Siniscalchi	Technical University of Denmark, Denmark
Daniel Slamanig	Austrian Institute of Technology, Austria
Jill Slay	University of South Australia, Australia
Willy Susilo	University of Wollongong, Australia
Vanessa Teague	Australian National University, Australia
Ding Wang	Nankai University, China
Huaxiong Wang	Nanyang Technological University, Singapore
Guomin Yang	Singapore Management University, Singapore
Yuval Yarom	University of Adelaide, Australia
Xun Yi	RMIT University, Australia
Quan Yuan	University of Tokyo, Japan
Tsz Hon Yuen	University of Hong Kong, Hong Kong

External Reviewers

Léo Ackermann	Xingye Lu
Kanwal Aslam Syed	Tran Ngo
Sepideh Avizheh	Cong Peng
Syed Badruddoja	Octavio Pérez-Kempner
Anuhbab Baksi	Simone Perriello
Priyanka Dutta	Lucas Prabel
Sabyasachi Dutta	Sebastian Ramacher
Jonathan Eriksen	Krijn Reijnders
Rami Haffar	Partha Sarathi Roy
Preston Haffey	Syh-Yuan Tan
Pavol Helebrandt	Sulani Thakshila
Kai Hu	Monika Trimoska
Ryoma Ito	Peng Wang
Hansraj Jangir	Kexin Xu
Dingding Jia	Yanhong Xu
Yinhao Jiang	Haiyang Xue
Elena Kirshanova	Xiao Yang
Jiahao Liu	Liu Zhang
Jinyu Lu	Yafei Zheng

Local Organizing Committee Chairs

Leonie Simpson	Queensland University of Technology, Australia
Mir Ali Rezazadeh Bae	Queensland University of Technology, Australia

Contents

Symmetric-Key Cryptography

Improved Differential Cryptanalysis on SPECK Using Plaintext Structures	3
<i>Zhuohui Feng, Ye Luo, Chao Wang, Qianqian Yang, Zhiquan Liu, and Ling Song</i>	
Linear Cryptanalysis and Its Variants with Fast Fourier Transformation Technique on MPC/FHE/ZK-Friendly \mathbb{F}_p -Based Ciphers	25
<i>Zeyu Xu, Shiyao Chen, Meiqin Wang, and Puwen Wei</i>	
A New Correlation Cube Attack Based on Division Property	53
<i>Cheng Che and Tian Tian</i>	
The Triangle Differential Cryptanalysis	72
<i>Xiaofeng Xie and Tian Tian</i>	
Key Recovery Attacks on Grain-Like Keystream Generators with Key Injection	89
<i>Matthew Beighton, Harry Bartlett, Leonie Simpson, and Kenneth Koon-Ho Wong</i>	
Related-Cipher Attacks: Applications to Ballet and ANT	109
<i>Yongxia Mao, Wenling Wu, Yafei Zheng, and Lei Zhang</i>	
Cryptanalysis of SPEEDY	124
<i>Jinliang Wang, Chao Niu, Qun Liu, Muzhou Li, Bart Preneel, and Meiqin Wang</i>	
Reconsidering Generic Composition: The Modes A10, A11 and A12 are Insecure	157
<i>Francesco Berti</i>	
Exploring Formal Methods for Cryptographic Hash Function Implementations	177
<i>Nicky Mouha</i>	

Public-Key Cryptography

A Tightly Secure ID-Based Signature Scheme Under DL Assumption in AGM	199
<i>Jia-Chng Loh, Fuchun Guo, Willy Susilo, and Guomin Yang</i>	
Compact Password Authenticated Key Exchange from Group Actions	220
<i>Ren Ishibashi and Kazuki Yoneyama</i>	
Multi-key Homomorphic Secret Sharing from LWE Without Multi-key HE	248
<i>Peiying Xu and Li-Ping Wang</i>	
Identity-Based Encryption from Lattices Using Approximate Trapdoors	270
<i>Malika Izabachène, Lucas Prabel, and Adeline Roux-Langlois</i>	
Homomorphic Signatures for Subset and Superset Mixed Predicates and Its Applications	291
<i>Masahito Ishizaka and Kazuhide Fukushima</i>	
Adaptively Secure Identity-Based Encryption from Middle-Product Learning with Errors	320
<i>Jingjing Fan, Xingye Lu, and Man Ho Au</i>	

Post-Quantum Cryptography

Quantum-Access Security of Hash-Based Signature Schemes	343
<i>Quan Yuan, Mehdi Tibouchi, and Masayuki Abe</i>	
Tightly Secure Lattice Identity-Based Signature in the Quantum Random Oracle Model	381
<i>Ernest Foo and Qinyi Li</i>	
Ghidle: Efficient Large-State Block Ciphers for Post-quantum Security	403
<i>Motoki Nakahashi, Rentaro Shiba, Ravi Anand, Mostafizar Rahman, Kosei Sakamoto, Fukang Liu, and Takanori Isobe</i>	
Quantum Algorithm for Finding Impossible Differentials and Zero-Correlation Linear Hulls of Symmetric Ciphers	431
<i>Huiqin Chen, Yongqiang Li, Parhat Abla, Zhiran Li, Lin Jiao, and Mingsheng Wang</i>	
Memory-Efficient Quantum Information Set Decoding Algorithm	452
<i>Naoto Kimura, Atsushi Takayasu, and Tsuyoshi Takagi</i>	

Cryptographic Protocols

CSI-SharK: CSI-FiSh with Sharing-friendly Keys	471
<i>Shahla Atapoor, Karim Baghery, Daniele Cozzo, and Robi Pedersen</i>	
Practical Verifiable Random Function with RKA Security	503
<i>Tsz Hon Yuen, Shimin Pan, Sheng Huang, and Xiaoting Zhang</i>	
Statistically Consistent Broadcast Authenticated Encryption with Keyword Search: Adaptive Security from Standard Assumptions	523
<i>Sayantan Mukherjee</i>	
Modular Design of KEM-Based Authenticated Key Exchange	553
<i>Colin Boyd, Bor de Kock, and Lise Millerjord</i>	
Reusable, Instant and Private Payment Guarantees for Cryptocurrencies	580
<i>Akash Madhusudan, Mahdi Sedaghat, Samarth Tiwari, Kelong Cong, and Bart Preneel</i>	

System Security

BinAlign: Alignment Padding Based Compiler Provenance Recovery	609
<i>Maliha Ismail, Yan Lin, DongGyun Han, and Debin Gao</i>	
Encrypted Network Traffic Classification with Higher Order Graph Neural Network	630
<i>Zulu Okonkwo, Ernest Foo, Zhe Hou, Qinyi Li, and Zahra Jadidi</i>	
Author Index	651