Lecture Notes in Computer Science 13083

Founding Editors

Gerhard Goos
Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis
Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino
Purdue University, West Lafayette, IN, USA

Wen Gao
Peking University, Beijing, China

Bernhard Steffen
TU Dortmund University, Dortmund, Germany

Gerhard Woeginger
RWTH Aachen, Aachen, Germany

Moti Yung
Columbia University, New York, NY, USA

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

Joonsang Baek · Sushmita Ruj (Eds.)

Information Security and Privacy

26th Australasian Conference, ACISP 2021
Virtual Event, December 1–3, 2021
Proceedings

Springer

Editors
Joonsang Baek
University of Wollongong
Wollongong, NSW, Australia

Sushmita Ruj
Data61, CSIRO
Marsfield, NSW, Australia

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-90566-8 ISBN 978-3-030-90567-5 (eBook)
https://doi.org/10.1007/978-3-030-90567-5

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021
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

It is our great pleasure to present the proceedings of ACISP 2021, the 26th Australasian Conference on Information Security and Privacy, held virtually during December 1–3, 2021.

ACISP was first held at the University of Wollongong in 1996 and since then has been organized in various cities in Australia and New Zealand — Wollongong (1996, 1999, 2003, 2008, 2012, 2014, 2018), Sydney (1997, 2001, 2004, 2010), Melbourne (2002, 2006, 2011, 2016), Brisbane (1998, 2000, 2005, 2009, 2013, 2015), Townsville (2007), Auckland (2017), Christchurch (2019). This annual event has gained its place among prestigious security and privacy conferences in the world. Due to the COVID-19 pandemic, and like last year, this year's ACISP was a virtual event.

ACISP 2021 attracted 157 submissions. All papers were reviewed by at least three reviewers. The double-blind review phase was followed by a fortnight-long discussion period that generated additional comments from the Program Committee members and the external reviewers. After the discussions, and after shepherding in a few cases, 35 papers were accepted for inclusion in the program. These 35 papers were presented during the conference, and revised versions of these papers are included in these proceedings. Two special sessions on Blockchains and Machine Learning Security and Privacy were organized to encourage researchers to participate in these cutting-edge areas.

Among the accepted papers, the paper with the highest weighted review mark received the Best Paper Award: Concise Mercurial Subvector Commitments: Definitions and Constructions by Yannan Li, Willy Susilo, Guomin Yang, Tran Viet Xuan Phuong, Yong Yu, and Dongxi Liu.

The conference would not have been possible without the hard work of the 60 Program Committee members from 18 different countries and the 126 external reviewers, who took part in the process of reviewing and subsequent discussions. We take this opportunity to thank the Program Committee members and the external reviewers for their tremendous job resulting in this year's program. It has been an honour to work with them. We would also like to express our appreciation to Springer for their active cooperation and timely production of these conference proceedings. In addition to the technical talks, the program included keynote talks and a panel discussion.

Finally, we would like to thank all the authors who submitted their work to ACISP 2021, and all the information security and privacy practitioners and enthusiasts who attended the event. Without your spirited participation, the conference would not be a success.

December 2021

Joonsang Baek
Sushmita Ruj

Organization

General Chairs

Hui Cui	Murdoch University, Australia
Joseph Liu	Monash University, Australia
Surya Nepal	CSIRO's Data61, Australia

Program Committee Chairs

Joonsang Baek	University of Wollongong, Australia
Sushmita Ruj	CSIRO's Data61, Australia

Publication Chairs

Jongkil Kim	University of Wollongong, Australia
Yannan Li	University of Wollongong, Australia

Registration Chair

Xingliang Yuan	Monash University, Australia

Web Chair

Raj Gaire	CSIRO's Data61, Australia

Program Committee

Shashank Agrawal	Western Digital Research, USA
Man Ho Au	University of Hong Kong, Hong Kong
Carsten Baum	Aarhus University, Denmark
Debrup Chakraborty	Indian Statistical Institute, Kolkata, India
Anupam Chattopadhyay	Nanyang Technological University, Singapore
Xiaofeng Chen	Xidian University, China
Rongmao Chen	National University of Defense Technology, China
Chitchanok Chuengsatiansup	University of Adelaide, Australia
Mauro Conti	University of Padua, Italy
Bernardo David	IT University of Copenhagen, Denmark
Dung Hoang Duong	University of Wollongong, Australia
Keita Emura	National Institute of Information and Communications Technology, Japan
Muhammed F. Esgin	Monash University and CSIRO's Data61, Australia

Ernest Foo	Griffith University, Australia
Chaya Ganesh	Indian Institute of Science, India
Mengmeng Ge	Deakin University, Australia
Esha Ghosh	Microsoft Research, USA
Vincent Gramoli	University of Sydney, Australia
Clémentine Gritti	University of Canterbury, New Zealand
Martin Hell	Lund University, Sweden
Swee-Huay Heng	Multimedia University, Malaysia
Sanjay Jha	University of New South Wales, Australia
Jinguang Han	Queen's University Belfast, UK
Dongseong Kim	University of Queensland, Australia
Hyoungshick Kim	Sungkyunkwan University, South Korea
Veronika Kuchta	University of Queensland, Australia
Jianchang Lai	Fujian Normal University, China
Jooyoung Lee	Korea Advanced Institute of Science and Technology, South Korea
Dongxi Liu	CSIRO's Data61, Australia
Rongxing Lu	University of New Brunswick, Canada
Siqi Ma	University of Queensland, Australia
Subhamoy Maitra	Indian Statistical Institute, India
Weizhi Meng	Technical Universtiy of Denmark, Denmark
Kirill Morozov	University of North Texas, USA
Khoa Nguyen	Nanyang Technological University, Singapore
Ariel Nof	Technion, Israel
Koji Nuida	Kyushu University, Japan
Elena Pagnin	Lund University, Sweden
Josef Pieprzyk	CSIRO's Data61, Australia, and Institute of Computer Science, PAN, Poland
Indrakshi Ray	Colorado State University, USA
Chester Rebeiro	Indian Institute of Technology, Madras, India
Partha Sarathi Roy	University of Wollongong, Australia
Reihaneh Safavi-Naini	University of Calgary, Canada
Sujoy Sinha Roy	Graz University of Technology, Austria
Kouichi Sakurai	Kyushu University, Japan
Amin Sakzad	Monash University, Australia
Pierangela Samarati	Università degli Studi di Milano, Italy
Binanda Sengupta	A*STAR, Singapore
Paul Stankovski Wagner	Lund University, Sweden
Qiang Tang	University of Sydney, Australia
Ni Trieu	Arizona State University, USA
Damien Vergnaud	Sorbonne Université and Institut Universitaire de France, France
Cong Wang	City University of Hong Kong, Hong Kong
Minhui Xue	University of Adelaide, Australia
Hailun Yan	EPFL, Switzerland
Yuval Yarom	University of Adelaide and CSIRO's Data61, Australia

Xun Yi	RMIT University, Australia
Siu Ming Yiu	University of Hong Kong, Hong Kong
Tsz Hon Yuen	University of Hong Kong, Hong Kong
Jianying Zhou	Singapore University of Technology and Design, Singapore

Additional Reviewers

Mohsen Ali
Kazumaro Aoki
Sepideh Avizheh
Syed Badruddoja
Samiran Bag
Anubhab Baksi
Subhadeep Banik
James Bartusek
Andrea Basso
Rouzbeh Behnia
Jakub Breier
Carlo Brunetta
Andrea Caforio
Cailing Cai
Marco Calderini
Stefano Cecconello
Fateme Hashemi Chaleshtori
Donghoon Chang
Nandish Chattopadhyay
Jinrong Chen
Joo Yeon Cho
Sherman S. M. Chow
Daniel Collins
Handong Cui
Sumit Kumar Debnath
Ioannis Demertzis
Sabyasachi Dutta
Maryam Ehsanpour
Batnyam Enkhtaivan
Oguzhan Ersoy
Jiahui Gao
Lorenzo Gentile
Hossein Ghodosi
Satrajit Ghosh
Sudipto Ghosh
Naina Gupta
Deukjo Hong
Kai Hu
Loïs Huguenin-Dumittan
Shaoquan Jiang
Yuting Jiang
Yoshiaki Kasahara
He Ke
Andrei Kelarev
Shabnam Kasra Kermanshahi
Mustafa Khairallah
Duhyeong Kim
Intae Kim
Ravi Kishore
Hiroshi Koide
Piotr Kokoszka
Venkata Koppula
Anders Konring
Gulshan Kumar
Shangqi Lai
Jason LeGrow
Mario Larangeira
Ngoc Le
Qinyi Li
Shuaigang Li
Xinyu Li
Zengpeng Li
Bowen Liu
Jia-Chng Loh
Daniel Masny
Alexander Munch-Hansen
Dukjae Moon
Pawel Morawiecki
Jianting Ning
Ngoc Khanh Nguyen
Satsuya Ohata
Shimin Pan
Bo Pang
Upakar Paudel

Russell Paulet
Rahul Rachuri
Xianrui Qin
Srinivasan Raghuraman
Prasanna Ravi
Rahul Saha
Rajeev Anand Sahu
Iftekhar Salam
Subhabrata Samajder
Santanu Sarkar
Sina Mahdipour Saravani
Gaurav Sharma
Jun Shen
Kazumasa Shinagawa
Hossein Shirazi
Tjerand Silde
Siang Meng Sim
Leonie Simpson
Mohit Singh
Nikhilesh Kumar Singh
Aikaterini Sotiraki
Jiawei Su
Chetan Surana
Siwei Sun
Haowen Tan
Syhyuan Tan
Teik Guan Tan
Guohua Tian
Yangguang Tian
Kritagya Upadhyay
Shannon Veitch
Dai Watanabe
Mingli Wu
Zhihua Xia
Yi Xie
Rui Xu
Rupeng Yang
Chia-Mu Yu
Xu Yang
Xuechao Yang
Zhichao Yang
Yacheng Wang
Yi Wang
Zheng Yang
Wei-Chuen Yau
Neng Zeng
Raymond Zhao
Yunlei Zhao
Xiaoyu Zhang
Fei Zhu
Rahman Ziaur
Cong Zuo

Contents

Cryptographic Foundations

Leakage Resilient Cheating Detectable Secret Sharing Schemes 3
Sabyasachi Dutta and Reihaneh Safavi-Naini

Chosen Ciphertext Secure Functional Encryption from Constrained Witness PRF 24
Tapas Pal and Ratna Dutta

Updatable Trapdoor SPHFs: Modular Construction of Updatable Zero-Knowledge Arguments and More 46
Behzad Abdolmaleki and Daniel Slamanig

Small Superset and Big Subset Obfuscation 68
Steven D. Galbraith and Trey Li

Symmetric Primitives

Algebraic Attacks on Round-Reduced Keccak 91
Fukang Liu, Takanori Isobe, Willi Meier, and Zhonghao Yang

On MILP-Based Automatic Search for Bit-Based Division Property for Ciphers with (Large) Linear Layers 111
Muhammad ElSheikh and Amr M. Youssef

Constructions of Iterative Near-MDS Matrices with the Lowest XOR Count 132
Xiaodan Li and Wenling Wu

Forced Independent Optimized Implementation of 4-Bit S-Box 151
Yanhong Fan, Weijia Wang, Zhihu Li, Zhenyu Lu, Siu-Ming Yiu, and Meiqin Wang

Distinguishing and Key Recovery Attacks on the Reduced-Round SNOW-V 171
Jin Hoki, Takanori Isobe, Ryoma Ito, Fukang Liu, and Kosei Sakamoto

Encryption

Broadcast Authenticated Encryption with Keyword Search 193
Xueqiao Liu, Kai He, Guomin Yang, Willy Susilo, Joseph Tonien, and Qiong Huang

An Anonymous Trace-and-Revoke Broadcast Encryption Scheme 214
Olivier Blazy, Sayantan Mukherjee, Huyen Nguyen, Duong Hieu Phan, and Damien Stehlé

Security Analysis of End-to-End Encryption for Zoom Meetings. 234
Takanori Isobe and Ryoma Ito

CCA Secure Attribute-Hiding Inner Product Encryption from Minimal Assumption 254
Tapas Pal and Ratna Dutta

Privacy

Optimal Randomized Partial Checking for Decryption Mix Nets 277
Thomas Haines and Johannes Müller

A Novel Proof of Shuffle: Exponentially Secure Cut-and-Choose 293
Thomas Haines and Johannes Müller

Private Decision Tree Evaluation with Constant Rounds via (Only) Fair SS-4PC 309
Hikaru Tsuchida and Takashi Nishide

Partially-Fair Computation from Timed-Release Encryption and Oblivious Transfer 330
Geoffroy Couteau, A. W. Roscoe, and Peter Y. A. Ryan

Blockchain - Protocols and Foundations

Concise Mercurial Subvector Commitments: Definitions and Constructions 353
Yannan Li, Willy Susilo, Guomin Yang, Tran Viet Xuan Phuong, Yong Yu, and Dongxi Liu

A Secure Cross-Shard View-Change Protocol for Sharding Blockchains. 372
Yizhong Liu, Jianwei Liu, Yiming Hei, Yu Xia, and Qianhong Wu

Efficient Unique Ring Signature for Blockchain Privacy Protection 391
Anh The Ta, Thanh Xuan Khuc, Tuong Ngoc Nguyen, Huy Quoc Le, Dung Hoang Duong, Willy Susilo, Kazuhide Fukushima, and Shinsaku Kiyomoto

Redactable Transactions in Consortium Blockchain: Controlled by Multi-authority CP-ABE 408
Zongyang Zhang, Tong Li, Zhuo Wang, and Jianwei Liu

Blockchain - Analysis and Attack

Transparency or Anonymity Leak: Monero Mining Pools Data Publication 433
Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld, and Dongxi Liu

Mind the Scraps: Attacking Blockchain Based on Selfdestruct 451
Wei-Yang Chiu and Weizhi Meng

Machine Learning for Privacy

A Blockchain-Enabled Federated Learning Model for Privacy Preservation: System Design 473
Minfeng Qi, Ziyuan Wang, Fan Wu, Rob Hanson, Shiping Chen, Yang Xiang, and Liming Zhu

ALRS: An Adversarial Noise Based Privacy-Preserving Data Sharing Mechanism 490
Jikun Chen, Ruoyu Deng, Hongbin Chen, Na Ruan, Yao Liu, Chao Liu, and Chunhua Su

Non-interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning 510
Carlo Brunetta, Georgia Tsaloli, Bei Liang, Gustavo Banegas, and Aikaterini Mitrokotsa

Machine Learning - Analysis and Attack

Towards Visualizing and Detecting Audio Adversarial Examples for Automatic Speech Recognition 531
Wei Zong, Yang-Wai Chow, and Willy Susilo

Oriole: Thwarting Privacy Against Trustworthy Deep Learning Models 550
Liuqiao Chen, Hu Wang, Benjamin Zi Hao Zhao, Minhui Xue, and Haifeng Qian

Post Quantum Cryptography - Encryption

Puncturable Identity-Based Encryption from Lattices 571
Priyanka Dutta, Willy Susilo, Dung Hoang Duong, and Partha Sarathi Roy

Optimizing Bootstrapping and Evaluating Large FHE Gates in the LWE-Based GSW-FHE 590
Chao Liu, Anyu Wang, and Zhongxiang Zheng

Forward-Secure Group Encryptions from Lattices 610
Jing Pan, Xiaofeng Chen, Fangguo Zhang, and Willy Susilo

Anonymous Lattice Identity-Based Encryption with Traceable Identities 630
Xavier Boyen, Ernest Foo, and Qinyi Li

Post Quantum Cryptography - Authentication

Lattice-Based Secure Biometric Authentication for Hamming Distance 653
Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, Joohee Lee, Junbum Shin, and Yongsoo Song

A Trustless GQ Multi-signature Scheme with Identifiable Abort 673
Handong Cui and Tsz Hon Yuen

Verifiable Obtained Random Subsets for Improving SPHINCS$^+$ 694
Mahmoud Yehia, Riham AlTawy, and T. Aaron Gulliver

Author Index 715