

Alastair R. Beresford
Arpita Patra
Emanuele Bellini (Eds.)

LNCs 13641

Cryptology and Network Security

21st International Conference, CANS 2022
Dubai, United Arab Emirates, November 13–16, 2022
Proceedings



Springer

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

Moti Yung 

Columbia University, New York, NY, USA


More information about this series at <https://link.springer.com/bookseries/558>


Alastair R. Beresford · Arpita Patra ·
Emanuele Bellini (Eds.)

Cryptology and Network Security

21st International Conference, CANS 2022
Dubai, United Arab Emirates, November 13–16, 2022
Proceedings

Editors

Alastair R. Beresford 
University of Cambridge
Cambridge, UK

Arpita Patra 
Indian Institute of Science
Bangalore, India

Emanuele Bellini 
Cryptography Research Center
Technology Innovation Institute
Abu Dhabi, United Arab Emirates

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-20973-4

ISBN 978-3-031-20974-1 (eBook)

<https://doi.org/10.1007/978-3-031-20974-1>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

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

The 21st International Conference on Cryptology and Network Security (CANS 2022) was held in Abu Dhabi during November 13–16, 2022.

CANS is an established annual conference presenting novel research work on cryptography, computer and network security, data security and privacy. Previous editions of CANS were held in Taipei (2001), San Francisco (2002), Miami (2003), Xiamen (2005), Suzhou (2006), Singapore (2007), Hong Kong (2008), Kanazawa (2009), Kuala Lumpur (2010), Sanya (2011), Darmstadt (2012), Parary (2013), Crete (2014), Marrakesh (2015), Milan (2016), Hong Kong (2017), Naples (2018), Fuzhou (2019) and virtually due to COVID-19 (2020, 2021).

In 2022 we received 54 submissions, out of which 18 full papers and two short papers were accepted for publication. We used a double-blind review process with three reviews per submission. The Program Committee chairs handled conflicts and used written reviews as well as online discussion with the reviewers to select the papers included in these proceedings. All authors were given the opportunity to revise their papers in response to reviewer feedback; a few papers were assigned a member of the Program Committee as a shepherd to support this process.

We would like to thank the Technology Innovation Institute (TII) for their support during the planning and running of the conference as well as Springer for their assistance in the production of the proceedings. We are extremely grateful to all the authors of the submitted papers as well as the 45 Program Committee members and 23 external reviewers for their care and dedication. Finally, we would like to thank the steering committee and organizing committee for their support and encouragement.

September 2022

Alastair R. Beresford
Arpita Patra
Emanuele Bellini

Organization

General Chair

Emanuele Bellini

Technology Innovation Institute, UAE

Program Committee Chairs

Alastair R. Beresford

University of Cambridge, UK

Arpita Patra

Indian Institute of Science Bangalore, India

Steering Committee

Yvo G. Desmedt (Chair)

University of Texas at Dallas, USA

Juan A. Garay

Texas A&M University, USA

Yi Mu

Fujian Normal University, China

Panos Papadimitratos

KTH Royal Institute of Technology, Sweden

David Pointcheval

CNRS and ENS Paris, France

Huaxiong Wang

Nanyang Technological University, Singapore

Organizing Committee

Emanuele Bellini

Technology Innovation Institute, UAE

Ana Castillo

Technology Innovation Institute, UAE

Program Committee

Cristina Alcaraz

University of Malaga, Spain

Subhadeep Banik

École Polytechnique Fédérale de Lausanne
(EPFL), Switzerland

Emanuele Bellini

Technology Innovation Institute, UAE

Arka Rai Choudhury

University of California, Berkeley, USA

Sherman Chow

Chinese University of Hong Kong, Hong Kong

Sandro Coretti-Drayton

Input Output Hong Kong (IOHK), Switzerland

Bernardo David

IT University of Copenhagen (ITU), Denmark

F. Betül Durak

Microsoft Research, USA

Pooya Farshim

Durham University, UK

Chaya Ganesh

Indian Institute of Science Bangalore, India

Satrajit Ghosh

IIT Kharagpur, India

Ariel Hamlin	MIT Lincoln Laboratory, USA
Panagiotis Ilia	University of Illinois, USA
Tetsu Iwata	Nagoya University, Japan
Ashwin Jha	CISPA Helmholtz Center for Information Security, Germany
Martin Kleppmann	University of Cambridge, UK
Ivan Martionvic	University of Oxford, UK
René Mayrhofer	Johannes Kepler University Linz, Austria
Veelasha Moonsamy	Ruhr University Bochum, Germany
Mridul Nandi	Indian Statistical Institute, India
Guevara Noubir	Northeastern University, USA
Emmanuela Orsini	Katholieke Universiteit (KU) Leuven, Belgium
Sergio Pastrana	Universidad Carlos III de Madrid, Spain
Sikhar Patranabis	IBM Research India, India
Constantinos Patsakis	University of Piraeus, Greece
Somitra Sanadhya	IIT Jodhpur, India
Dominique Schroder	University of Erlangen-Nuremberg, Germany
Mridula Singh	CISPA Helmholtz Center for Information Security, Germany
Alberto Sonnino	Mysten Labs, UK
Angelo Spognardi	Sapienza Università di Roma, Italy
Christoph Striecks	AIT Austrian Institute of Technology, Austria
Ajith Suresh	Technische Universität Darmstadt, Germany
Willy Susilo	University of Wollongong, Australia
Daniel Tschudi	Concordium, Switzerland
Giorgos Vasiliadis	FORTH and Hellenic Mediterranean University, Greece
Damien Vergnaud	LIP6, Sorbonne Université, France
João Vilela	University of Porto, Portugal
Corrado Aaron Visaggio	University of Sannio, Italy
Isabel Wagner	De Montfort University, UK
Huaxiong Wang	Nanyang Technological University, Singapore
Edgar Weippl	University of Vienna, Austria
Xingliang Yuan	Monash University, Australia
Zhenfei Zhang	Ethereum Foundation, USA

Additional Reviewers

Navid Alamati	Mariana Cunha
Khashayar Barooti	Avijit Dutta
Suvradip Chakraborty	Loïs Huguenin-Dumittan
Gwangbae Choi	Amit Jana
Daniel Collins	Matthias J. Kannwischer

Shangqi Lai
Benjamin Lipp
Omid Mir
Munkenyi Mukhandi
Rahul Rachuri
Gerald Schoiber
Karl Southern

Erkan Tairi
Serge Vaudenay
Dabao Wang
Harry W. H. Wong
Bang Wu
Huangting Wu

Contents

Zero-Knowledge and MPC

Efficient NIZK Arguments with Straight-Line Simulation and Extraction	3
<i>Michele Ciampi and Ivan Visconti</i>	
Updatable NIZKs from Non-Interactive Zaps	23
<i>Karim Bagheri and Navid Ghaedi Bardeh</i>	
Through the Looking-Glass: Benchmarking Secure Multi-party Computation Comparisons for ReLU 's	44
<i>Abdelrahman Aly, Kashif Nawaz, Eugenio Salazar, and Victor Sucasas</i>	

Public-Key Infrastructure

Oh SSH-it, What's My Fingerprint? A Large-Scale Analysis of SSH Host Key Fingerprint Verification Records in the DNS	71
<i>Sebastian Neef and Nils Wisiol</i>	
Attribute-Based Anonymous Credential: Optimization for Single-Use and Multi-Use	89
<i>Kwan Yin Chan and Tsz Hon Yuen</i>	
Auditable Asymmetric Password Authenticated Public Key Establishment	122
<i>Antonio Faonio, Maria Isabel Gonzalez Vasco, Claudio Soriente, and Hien Thi Thu Truong</i>	
(Augmented) Broadcast Encryption from Identity Based Encryption with Wildcard	143
<i>Anaïs Barthoulot, Olivier Blazy, and Sébastien Canard</i>	

Attacks and Countermeasures

Passive Triangulation Attack on ORide	167
<i>Shyam Murthy and Srinivas Vivek</i>	
HyperDetector: Detecting, Isolating, and Mitigating Timing Attacks in Virtualized Environments	188
<i>Musa Sadik Unal, Arsalan Javeed, Cemal Yilmaz, and Erkey Savas</i>	

Cryptanalysis and Provable Security

The Construction and Application of (Related-Key) Conditional
Differential Neural Distinguishers on KATAN 203
Dongdong Lin, Shaozhen Chen, Manman Li, and Zezhou Hou

How to Design Authenticated Key Exchange for Wearable Devices:
Cryptanalysis of AKE for Health Monitoring and Countermeasures
via Distinct SMs with Key Split and Refresh 225
Łukasz Krzywiecki and Hannes Salin

Cryptanalysis of the Multi-Power RSA Cryptosystem Variant 245
Didier Alquié, Guy Chassé, and Abderrahmane Nitaj

Provable Security of HADES Structure 258
Yuan Gao and Chun Guo

Cryptographic Protocols

Practical Single-Pass Oblivious Aggregation and Billing Computation
Protocols for Smart Meters 279
Kalikinkar Mandal

Anonymous Random Allocation and Its Applications 292
Azam Soleimanian

ACDC: Anonymous Crowdsourcing Using Digital Cash 314
Luis A. Saavedra and Alastair R. Beresford

Blockchain and Payment Systems

Analyzing Price Deviations in DeFi Oracles 329
Ankit Gangwal, Rahul Valluri, and Mauro Conti

Redacting Blockchain Without Exposing Chameleon Hash Collisions 339
Thiago Leucz Astrizi and Ricardo Custódio

Codes and Post-quantum Cryptography

Efficient Proofs of Retrievability Using Expander Codes 361
Françoise Levy-dit-Vehel and Maxime Roméas

Post-Quantum Electronic Identity: Adapting OpenID Connect and OAuth 2.0 to the Post-Quantum Era	371
<i>Frederico Schardong, Alexandre Augusto Giron, Fernanda Larisa Müller, and Ricardo Custódio</i>	
Author Index	391