

Mauro Conti
Marc Stevens
Stephan Krenn (Eds.)

LNCS 13099

Cryptology and Network Security

20th International Conference, CANS 2021
Vienna, Austria, December 13–15, 2021
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

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this subseries at <https://link.springer.com/bookseries/7410>

Mauro Conti · Marc Stevens ·
Stephan Krenn (Eds.)

Cryptology and Network Security

20th International Conference, CANS 2021
Vienna, Austria, December 13–15, 2021
Proceedings

Editors

Mauro Conti 
University of Padua
Padua, Italy

Marc Stevens 
Centrum Wiskunde & Informatica
Amsterdam, The Netherlands

Stephan Krenn 
AIT Austrian Institute of Technology
Vienna, Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-92547-5 ISBN 978-3-030-92548-2 (eBook)
<https://doi.org/10.1007/978-3-030-92548-2>

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

The 20th International Conference on Cryptology and Network Security (CANS 2021) was held during December 13–15, 2021. CANS 2021 was held in cooperation with the International Association for Cryptologic Research (IACR) and the AIT Austrian Institute of Technology. Due to the ongoing COVID-19 pandemic, CANS 2021 was held as a virtual conference, instead of at the intended venue in Vienna, Austria.

CANS is a recognized annual conference focusing on cryptology, computer and network security, and data security and privacy, attracting cutting-edge research findings from scientists around the world. 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 (2020).

In 2021, the conference received 85 valid submissions. The submission and review process were completed using the EasyChair Web-based software system. We were helped by 30 Program Committee members and 63 external reviewers. The submissions went through a double-blind review process and 28 papers were selected. This volume collates the revised versions of the accepted papers. The Best Paper Award was given to the paper “Subversion-Resistant Quasi-Adaptive NIZK and Applications to Modular zk-SNARKs” by Behzad Abdolmaleki and Daniel Slamanig.

We would like to thank the AIT Austrian Institute of Technology, as well as the H2020 initiative CyberSec4Europe, for their support during the planning of the conference. We would also like to thank Springer for their support with producing the proceedings. We heartily thank the authors of all submitted papers. Moreover, we are grateful to the members of the Program Committee and the external sub-reviewers for their diligent work, as well as all members of the Organizing Committee for their kind help. We would also like to acknowledge the Steering Committee for supporting us.

October 2021

Mauro Conti
Marc Stevens
Stephan Krenn

Organization

Steering Committee

Yvo G. Desmedt (Chair)	University of Texas at Dallas, USA
Juan A. Garay	Texas A&M University, USA
Amir Herzberg	Bar-Ilan University, Israel
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

Program Committee Chairs

Mauro Conti	Università degli Studi di Padova, Italy
Marc Stevens	Centrum Wiskunde & Informatica (CWI), The Netherlands

General Chair

Stephan Krenn	AIT Austrian Institute of Technology, Austria
---------------	---

Organizing Committee

Alessandro Brighente	Università degli Studi di Padova, Italy
Manuela Kos	AIT Austrian Institute of Technology, Austria
Edgar Weippl	SBA Research and University of Vienna, Austria

Program Committee

Masayuki Abe	NTT, Japan
Cristina Alcaraz	University of Malaga, Spain
Lejla Batina	Radboud University, The Netherlands
Alastair Beresford	University of Cambridge, UK
Alessandro Brighente	University of Padua, Italy
Mauro Conti	University of Padua, Italy
Zekeriya Erkin	Delft University of Technology, The Netherlands
Peter Gaži	IOHK Research, Slovakia
Dieter Gollmann	Hamburg University of Technology, Germany
Sotiris Ioannidis	Technical University of Crete, Greece
Chhagan Lal	University of Padua, Italy
Riccardo Lazzeretti	Sapienza University of Rome, Italy

Eleonora Losiouk	University of Padua, Italy
Mark Manulis	University of Surrey, UK
Chris Mitchell	Royal Holloway, University of London, UK
Veelasha Moonsamy	Ruhr University Bochum, Germany
Gerardo Pelosi	Politecnico di Milano, Italy
Raphael C.-W. Phan	Monash University, Malaysia
Stjepan Picek	Delft University of Technology, The Netherlands
Sushmita Ruj	CSIRO, Data61, Australia
Dominique Schroeder	Friedrich-Alexander University Erlangen-Nürnberg, Germany
Angelo Spognardi	Sapienza University of Rome, Italy
Marc Stevens	Centrum Wiskunde & Informatica (CWI), The Netherlands
Thorsten Strufe	Karlsruhe Institute of Technology (KIT) and TU Dresden, Germany
Daniele Venturi	Sapienza University of Rome, Italy
Frederik Vercauteren	Katholieke Universiteit Leuven, Belgium
Damien Vergnaud	Université Pierre et Marie Curie and Institut Universitaire de France, France
Corrado Aaron Visaggio	University of Sannio, Italy
Edgar Weippl	University of Vienna, Austria
Chia-Mu Yu	National Chung Hsing University, Taiwan

Additional Reviewers

Hamza Abusalah	Maryam Ehsanpour
Kamalesh Acharya	Solane El Hirsch
Erdem Alkim	Francesco Felet
Miguel Ambrona	Danilo Francati
Francesco Antognazza	Jonathan Fuchs
Fatih Balli	Rafa Gálvez
Ward Beullens	Ankit Gangwal
Tim Beyne	Robert Granger
Sanjay Bhattacharjee	Bernhard Haslhofer
Hamid Bostani	Iliia Iliashenko
George Christou	Gulshan Kumar
Sandro Coretti	Russell W. F. Lai
Joan Daemen	Eftychia Lakka
F. W. Dekker	Mario Larangeira
Cyprien Delpech de Saint Guilhem	Julia Len
Dominic Deuber	Tianyu Li
Sabyasachi Dey	Jia Liu
Dimitris Deyannis	Philipp Markert
Michalis Diamantaris	Subhra Mazumdar
Sabyasachi Dutta	Alireza Mehrdad
Christoph Egger	Konstantina Miteloudi

Vinod P. Nair
Miyako Ohkubo
Guillermo Pascual-Perez
Robi Pedersen
Hilder Vitor Lima Pereira
Nikolaos Petroulakis
Md Masoom Rabbani
Viktoria Ronge
Paul Rösler
Rahul Saha
Simona Samardjiska

Laltu Sardar
Sruthi Sekar
Vojtech Suchanek
Titouan Tanguy
Cihangir Tezcan
Sri Aravinda Krishnan Thyagarajan
Meltem Sonmez Turan
Michiel Van Beirendonck
Jelle Vos
Florian Weber

Contents

Encryption

Cross-Domain Attribute-Based Access Control Encryption	3
<i>Mahdi Sedaghat and Bart Preneel</i>	
Grain-128AEADv2: Strengthening the Initialization Against Key Reconstruction	24
<i>Martin Hell, Thomas Johansson, Alexander Maximov, Willi Meier, and Hirotaka Yoshida</i>	
Partition Oracles from Weak Key Forgeries	42
<i>Marcel Armour and Carlos Cid</i>	
Practical Privacy-Preserving Face Identification Based on Function-Hiding Functional Encryption	63
<i>Alberto Ibarrondo, Hervé Chabanne, and Melek Önen</i>	
The Matrix Reloaded: Multiplication Strategies in FrodoKEM	72
<i>Jooppe W. Bos, Maximilian Ofner, Joost Renes, Tobias Schneider, and Christine van Vredendaal</i>	

Signatures

BlindOR: an Efficient Lattice-Based Blind Signature Scheme from OR-Proofs	95
<i>Nabil Alkeilani Alkadri, Patrick Harasser, and Christian Janson</i>	
Efficient Threshold-Optimal ECDSA	116
<i>Michaella Pettit</i>	
GM ^{MT} : A Revocable Group Merkle Multi-tree Signature Scheme	136
<i>Mahmoud Yehia, Riham AlTawy, and T. Aaron Gulliver</i>	
Issuer-Hiding Attribute-Based Credentials	158
<i>Jan Bobolz, Fabian Eidens, Stephan Krenn, Sebastian Ramacher, and Kai Samelin</i>	
Report and Trace Ring Signatures	179
<i>Ashley Fraser and Elizabeth A. Quaglia</i>	

Selectively Linkable Group Signatures—Stronger Security and Preserved Verifiability 200
Ashley Fraser, Lydia Garms, and Anja Lehmann

Cryptographic Schemes and Protocols

FO-like Combiners and Hybrid Post-Quantum Cryptography 225
Lois Huguenin-Dumittan and Serge Vaudenay

Linear-Time Oblivious Permutations for SPDZ 245
Peeter Laud

On the Higher-Bit Version of Approximate Inhomogeneous Short Integer Solution Problem 253
Anaëlle Le Dévéhat, Hiroki Shizuya, and Shingo Hasegawa

Practical Continuously Non-malleable Randomness Encoders in the Random Oracle Model 273
Antonio Faonio

Attacks and Counter-Measures

Countermeasures Against Backdoor Attacks Towards Malware Detectors 295
Shintaro Narisada, Yuki Matsumoto, Seira Hidano, Toshihiro Uchibayashi, Takuo Suganuma, Masahiro Hiji, and Shinsaku Kiyomoto

Free by Design: On the Feasibility of Free-Riding Attacks Against Zero-Rated Services 315
Julian Fietkau, David Pascal Runge, and Jean-Pierre Seifert

Function-Private Conditional Disclosure of Secrets and Multi-evaluation Threshold Distributed Point Functions 334
Nolan Miranda, Foo Yee Yeo, and Vipin Singh Sehrawat

How Distance-Bounding Can Detect Internet Traffic Hijacking 355
Ghada Arfaoui, Gildas Avoine, Olivier Gimenez, and Jacques Traoré

SoK: Secure Memory Allocation 372
Bojan Novković and Marin Golub

Toward Learning Robust Detectors from Imbalanced Datasets Leveraging Weighted Adversarial Training 392
Kento Hasegawa, Seira Hidano, Shinsaku Kiyomoto, and Nozomu Togawa

Towards Quantum Large-Scale Password Guessing on Real-World Distributions 412
Markus Dürmuth, Maximilian Golla, Philipp Markert, Alexander May, and Lars Schlieper

Attestation and Verification

Anonymous Transactions with Revocation and Auditing in Hyperledger Fabric 435
Dmytro Bogatov, Angelo De Caro, Kaoutar Elkhiyaoui, and Björn Tackmann

Attestation Waves: Platform Trust via Remote Power Analysis 460
Ignacio M. Delgado-Lozano, Macarena C. Martínez-Rodríguez, Alexandros Bakas, Billy Bob Brumley, and Antonis Michalas

How (not) to Achieve both Coercion Resistance and Cast as Intended Verifiability in Remote eVoting 483
Tamara Finogina, Javier Herranz, and Enrique Larraia

Subversion-Resistant Quasi-adaptive NIZK and Applications to Modular Zk-SNARKs 492
Behzad Abdolmaleki and Daniel Slamanig

THC: Practical and Cost-Effective Verification of Delegated Computation 513
Pablo Rauzy and Ali Nehme

TIRAMISU: Black-Box Simulation Extractable NIZKs in the Updatable CRS Model 531
Karim Baghery and Mahdi Sedaghat

Author Index 553