

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>

Steven D. Galbraith (Ed.)

Topics in Cryptology – CT-RSA 2022

Cryptographers' Track at the RSA Conference 2022
Virtual Event, March 1–2, 2022
Proceedings

Editor

Steven D. Galbraith 
University of Auckland
Auckland, New Zealand

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-95311-9

ISBN 978-3-030-95312-6 (eBook)

<https://doi.org/10.1007/978-3-030-95312-6>

LNCS Sublibrary: SL4 – Security and Cryptology

© 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 RSA conference has been a major international event for information security experts since its inception in 1991. It is an annual event that attracts several hundred vendors and over 40,000 participants from industry, government, and academia. Since 2001, the RSA conference has included the Cryptographers' Track (CT-RSA). This track, essentially a sub-conference of the main event, provides a forum for the dissemination of current research in cryptography. This volume represents the proceedings of the 2022 edition of the Cryptographers' Track at the RSA Conference.

On the original submission deadline there were 56 submissions. The deadline was extended by about 10 days and the final number of submissions was 87. As always, the selection process was challenging. The submissions were anonymous (double-blind review), and each submission was assigned to at least three reviewers. We followed the IACR policy on conflicts of interest. We used EasyChair for the submission and review process. At the conclusion of the review and discussion phase there were 20 accepted papers and five conditionally accepted papers. This is an acceptance rate of 28.7%. Subsequently one of the conditionally accepted papers was withdrawn by the authors, so the final conference program comprised 24 papers.

I am thankful to all Program Committee members for producing high-quality reviews and for actively participating in discussions. My appreciation also goes to all external reviewers. I am also grateful to those Program Committee members who checked the conditionally accepted submissions.

I am grateful to Kenny Paterson (the CT-RSA 2021 Program Chair) and Moti Yung (Chair of the CT-RSA Steering Committee) for their wisdom. I also thank Lukas Zobernig for setting up the conference webpage and for help with processing the final versions of the papers for publication.

This year the conference took place online as a virtual conference on March 1–2, 2022.

My sincere thanks go to the Springer team for their assistance in preparing and producing these proceedings. Last but not least, on behalf of all CT-RSA participants, I would like to thank Tara Jung and Britta Glade who acted as RSA Conference liaison to the Cryptographer's Track. I am very grateful to them for all the work they did in helping to organize both the in-person conference and also the online conference.

December 2021

Steven D. Galbraith

Organization

Program Chair

Steven D. Galbraith

University of Auckland, New Zealand

Program Committee

Masayuki Abe

NTT Laboratories, Japan

Gorjan Alagic

University of Maryland, USA

Man Ho Au

University of Hong Kong, Hong Kong

Shi Bai

Florida Atlantic University, USA

Paulo Barreto

University of Washington, USA

Lejla Batina

Radboud University, The Netherlands

Josh Benaloh

Microsoft Research, USA

Nina Bindel

University of Waterloo and Institute for Quantum Computing, Canada

Olivier Blazy

Ecole Polytechnique, France

Ran Cohen

Northeastern University, USA, and IDC Herzliya, Israel

Gareth T. Davies

Bergische Universität Wuppertal, Germany

Jean Paul Degabriele

TU Darmstadt, Germany

Prastudy Fauzi

Simula UiB, Bergen, Norway

Luca De Feo

IBM Research Europe – Zürich, Switzerland

Pierrick Gaudry

CNRS, Nancy, France

Qian Guo

Lund University, Sweden

Helena Handschuh

Rambus Cryptography Research, USA

Stanislaw Jarecki

University of California, Irvine, USA

Shuichi Katsumata

AIST, Japan

Marcel Keller

CSIRO Data61, Australia

Veronika Kuchta

University of Queensland, Australia

Joseph Liu

Monash University, Australia

Anna Lysyanskaya

Brown, USA

Giorgia Azzurra Marson

NEC Labs Europe, Germany

Willi Meier

University of Applied Sciences and Arts
Northwestern Switzerland (FHNW) Windisch,
Switzerland

Brice Minaud

Inria and ENS, France

Tarik Moataz

MongoDB, USA

Khoa Nguyen	Nanyang Technological University, Singapore, and University of Wollongong, Australia
Bertram Poettering	IBM Research Europe – Zürich, Switzerland
David Pointcheval	ENS, France
Bart Preneel	KU Leuven, Belgium
Mike Rosulek	Oregon State University, USA
Adeline Roux-Langlois	University of Rennes, CNRS, IRISA, France
Arnab Roy	University of Klagenfurt, Austria
Reihaneh Safavi-Naini	University of Calgary, Canada
Yu Sasaki	NTT Laboratories, Japan
Abhi Shelat	Northeastern University, USA
Luisa Siniscalchi	Aarhus University, Denmark
Nigel Smart	KU Leuven, Belgium
Willy Susilo	University of Wollongong, Australia
Qiang Tang	University of Sydney, Australia
Jacques Traoré	Orange Labs, France
Fernando Virdia	ETH Zürich, Switzerland

External Reviewers

Sepideh Avizheh	Vukašin Karadžić	Willy Quach
Ward Beullens	Yashvanth Kondi	Yuan Quan
Vincenzo Botta	Xinyu Li	Paul Rösler
Katharina Boudgoust	Fukang Liu	Partha Sarathi Roy
Maxime Buser	Xingye Lu	Rajeev Anand Sahu
Wouter Castryck	Lin Lyu	Olivier Sanders
Long Chen	Mark Marson	Peter Scholl
Liron David	Sarah McCarthy	Jan Schoone
Denis Diemert	Ian McQuoid	Gaurav Sharma
Jan Peter Drees	Marine Minier	Manasi Shingane
Abhraneel Dutta	Dustin Moody	Benjamin Smith
Thomas Espitau	Tran Ngo	Hadi Soleimany
Mojtaba Fadavi	Luca Notarnicola	Patrick Struck
Hanwen Feng	Arne Tobias Ødegaard	Zhimei Sui
Danilo Francati	Bo Pang	Anupama Unnikrishnan
Benedikt Gierlichs	Kenny Paterson	Michiel Van Beirendonck
Jérôme Govinden	Hilder V. L. Pereira	Haiyang Xue
Vincent Grosso	Jeroen Pijnenburg	Rupeng Yang
Martha Norberg Hovd	Lucas Prabel	Zuoxia Yu
Senyang Huang	Nitin Pundir	Shang Zehua
Floyd Johnson	Chen Qian	Yongjun Zhao

Contents

Multicast Key Agreement, Revisited	1
<i>Alexander Bienstock, Yevgeniy Dodis, and Yi Tang</i>	
A Pairing-Free Signature Scheme from Correlation Intractable Hash Function and Strong Diffie-Hellman Assumption	26
<i>Benoît Chevallier-Mames</i>	
Faster Isogenies for Post-quantum Cryptography: SIKE	49
<i>Rami Elkhatib, Brian Koziel, and Reza Azarderakhsh</i>	
Fully Projective Radical Isogenies in Constant-Time	73
<i>Jesús-Javier Chi-Domínguez and Krijn Reijnders</i>	
Private Liquidity Matching Using MPC	96
<i>Shahla Atapoor, Nigel P. Smart, and Younes Talibi Alaoui</i>	
Approximate Homomorphic Encryption with Reduced Approximation Error	120
<i>Andrey Kim, Antonis Papadimitriou, and Yuriy Polyakov</i>	
Attacks on Pseudo Random Number Generators Hiding a Linear Structure	145
<i>Florette Martinez</i>	
Lattice-Based Fault Attacks on Deterministic Signature Schemes of ECDSA and EdDSA	169
<i>Weiqiong Cao, Hongsong Shi, Hua Chen, Jiazhe Chen, Limin Fan, and Wenling Wu</i>	
More Accurate Geometric Analysis on the Impact of Successful Decryptions for IND-CCA Secure Ring/Mod-LWE/LWR Based Schemes	196
<i>Han Wu and Guangwu Xu</i>	
Integral Attacks on Pyjamask-96 and Round-Reduced Pyjamask-128	223
<i>Jiamin Cui, Kai Hu, Qingju Wang, and Meiqin Wang</i>	
Related-Tweakey Impossible Differential Attack on Reduced-Round SKINNY-AEAD M1/M3	247
<i>Yanhong Fan, Muzhou Li, Chao Niu, Zhenyu Lu, and Meiqin Wang</i>	

Side-Channeling the Kalyna Key Expansion	272
<i>Chitchanok Chuengsatiansup, Daniel Genkin, Yuval Yarom, and Zhiyuan Zhang</i>	
Fake It Till You Make It: Data Augmentation Using Generative Adversarial Networks for All the Crypto You Need on Small Devices	297
<i>Naila Mukhtar, Lejla Batina, Stjepan Picek, and Yinan Kong</i>	
A New Adaptive Attack on SIDH	322
<i>Tako Boris Fouotsa and Christophe Petit</i>	
On Fingerprinting Attacks and Length-Hiding Encryption	345
<i>Kai Gellert, Tibor Jager, Lin Lyu, and Tom Neuschulden</i>	
CCA Secure <i>A Posteriori</i> Openable Encryption in the Standard Model	370
<i>Xavier Bultel</i>	
Dynamic Universal Accumulator with Batch Update over Bilinear Groups	395
<i>Giuseppe Vitto and Alex Biryukov</i>	
Adaptively Secure Laconic Function Evaluation for NC^1	427
<i>Răzvan Roşie</i>	
FASTA – A Stream Cipher for Fast FHE Evaluation	451
<i>Carlos Cid, John Petter Indrøy, and Håvard Raddum</i>	
New Attacks from Old Distinguishers Improved Attacks on Serpent	484
<i>Marek Broll, Federico Canale, Nicolas David, Antonio Flórez-Gutiérrez, Gregor Leander, María Naya-Plasencia, and Yosuke Todo</i>	
Pholkos – Efficient Large-State Tweakable Block Ciphers from the AES Round Function	511
<i>Jannis Bossert, Eik List, Stefan Lucks, and Sebastian Schmitz</i>	
Robust Subgroup Multi-signatures for Consensus	537
<i>David Galindo and Jia Liu</i>	
Subversion-Resilient Enhanced Privacy ID	562
<i>Antonio Faonio, Dario Fiore, Luca Nizzardo, and Claudio Soriente</i>	

PriBank: Confidential Blockchain Scaling Using Short Commit-and-Proof NIZK Argument	589
<i>Kristian Gjøsteen, Mayank Raikwar, and Shuang Wu</i>	
Author Index	621