

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 series at <http://www.springer.com/series/7410>

Martin Albrecht (Ed.)

Cryptography and Coding

17th IMA International Conference, IMACC 2019
Oxford, UK, December 16–18, 2019
Proceedings

Editor
Martin Albrecht
Royal Holloway, University of London
London, UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-35198-4 ISBN 978-3-030-35199-1 (eBook)
<https://doi.org/10.1007/978-3-030-35199-1>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019

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 International Conference on Cryptography and Coding is the biennial conference of the Institute of Mathematics and its Applications (IMA) on cryptography and coding theory. The conference series has been running for more than three decades and the 17th edition was held December 16–18, 2019, at St Anne’s College, University of Oxford.

The Program Committee selected 17 submissions for presentation at the conference and inclusion in these proceedings. The review process was double-blind and rigorous. Each submission was reviewed independently by at least two reviewers in an individual review phase, and subsequently considered by the Program Committee in a discussion phase. Feedback from the reviews and discussions was given to the authors and their revised submissions are included in the proceedings.

In addition to the presentations of accepted papers, the conference also featured four keynote talks by internationally leading scientists on their research. I am grateful to Cas Cremers, Nadia Henninger, Clémentine Maurice, and Francesca Musiani for accepting our invitation and sharing the insights gathered from their exciting research. Finally, the conference featured several contributed presentations. However, these were not finalised by the time this preface went to print.

Running a conference like IMACC requires the effort of many people and many thanks are due. I would like to thank the Steering Committee for their trust and support. I thank the authors for their submissions and the Program Committee and the external reviewers for their effort in selecting the scientific program. Thanks also goes to the IACR for their cooperation. Finally, I am thankful to the conferences team – Maya Everson, Cerys Thompson, Pamela Bye, and colleagues – at the Institute of Mathematics and its Applications for handling all the practical matters of the conference.

September 2019

Martin Albrecht

Organization

Program Committee

Martin Albrecht	Royal Holloway, University of London, UK
Alex Davidson	Cloudflare Portugal, Portugal
Benjamin Dowling	ETH Zurich, Switzerland
Caroline Fontaine	CNRS (LSV), France
Julia Hesse	IBM Research Zurich, Switzerland
Christian Janson	TU Darmstadt, Germany
Cong Ling	Imperial College, UK
Emmanuela Orsini	Katholieke Universiteit Leuven, Belgium
Daniel Page	University of Bristol, UK
Christophe Petit	University of Oxford, UK
Rachel Player	Royal Holloway, University of London, UK
Elizabeth Quaglia	Royal Holloway, University of London, UK
Ciara Rafferty	Queen's University Belfast, UK
Christian Rechberger	TU Graz, Austria
Adeline Roux-Langlois	Univ Rennes, CNRS, IRISA, France
Christoph Striecks	AIT, Austria
Thyla van der Merwe	Mozilla, UK
Roope Vehkalahti	Aalto University, Finland
Carolyn Whitnall	University of Bristol, UK

Additional Reviewers

Bert, Pauline	Kwiatkowski, Kris
Costache, Ana	Martindale, Chloe
Dalskov, Anders	Merz, Simon-Philipp
Davies, Gareth	Persichetti, Edoardo
Dinur, Itai	Qian, Chen
Eaton, Edward	Ramacher, Sebastian
Fraser, Ashley	Renes, Joost
Garms, Lydia	Slamanig, Daniel
Gryak, Jonathan	van de Pol, Joop
Howe, James	Wen, Weiqiang
Kales, Daniel	Yu, Yang
Kutas, Peter	

Contents

A Framework for UC-Secure Commitments from Publicly Computable Smooth Projective Hashing.	1
<i>Behzad Abdolmaleki, Hamidreza Khoshakhlagh, and Daniel Slamanig</i>	
Subverting Decryption in AEAD.	22
<i>Marcel Armour and Bertram Poettering</i>	
Subversion-Resistant Simulation (Knowledge) Sound NIZKs	42
<i>Karim Baghery</i>	
Classification of Self-dual Codes of Length 20 over \mathbb{Z}_4 and Length at Most 18 over $\mathbb{F}_2 + u\mathbb{F}_2$	64
<i>Rowena Alma L. Betty and Akihiro Munemasa</i>	
A Framework for Universally Composable Oblivious Transfer from One-Round Key-Exchange	78
<i>Pedro Branco, Jintai Ding, Manuel Goulão, and Paulo Mateus</i>	
Efficient Fully Secure Leakage-Detering Encryption.	102
<i>Jan Camenisch, Maria Dubovitskaya, and Patrick Towa</i>	
Sharing the LUOV: Threshold Post-quantum Signatures.	128
<i>Daniele Cozzo and Nigel P. Smart</i>	
Commodity-Based 2PC for Arithmetic Circuits.	154
<i>Ivan Damgård, Helene Haagh, Michael Nielsen, and Claudio Orlandi</i>	
Improved Low-Memory Subset Sum and LPN Algorithms via Multiple Collisions.	178
<i>Claire Delaplace, Andre Esser, and Alexander May</i>	
Forgery Attacks on FlexAE and FlexAEAD.	200
<i>Maria Eichlseder, Daniel Kales, and Markus Schofnegger</i>	
Key Recovery Attacks on Some Rank Metric Code-Based Signatures	215
<i>Terry Shue Chien Lau, Chik How Tan, and Theo Fanuela Prabowo</i>	
On the Security of Multikey Homomorphic Encryption	236
<i>Hyang-Sook Lee and Jeongeun Park</i>	

RLWE-Based Zero-Knowledge Proofs for Linear and Multiplicative Relations	252
<i>Ramiro Martínez and Paz Morillo</i>	
Cryptanalysis of a Protocol for Efficient Sorting on SHE Encrypted Data. . . .	278
<i>Shyam Murthy and Srinivas Vivek</i>	
Quantum-Secure (Non-)Sequential Aggregate Message Authentication Codes.	295
<i>Shingo Sato and Junji Shikata</i>	
SO-CCA Secure PKE in the Quantum Random Oracle Model or the Quantum Ideal Cipher Model	317
<i>Shingo Sato and Junji Shikata</i>	
Distributing Any Elliptic Curve Based Protocol	342
<i>Nigel P. Smart and Younes Talibi Alaoui</i>	
Author Index	367