Lecture Notes in Computer Science 11929

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

Springer

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

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

Contents