

# 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 16th edition was held December 12–14 at St. Catherine’s College, University of Oxford. We received 32 submissions from authors all over the world on a diverse set of topics both in cryptography and coding theory. The Program Committee selected 19 of the submissions for presentation at the conference. 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 in the interface of cryptography and coding theory. I am grateful to Daniele Micciancio, Jan Camenisch, Nicolas Sendrier, and Thomas Prest for accepting our invitation and sharing the insights gathered from their exciting research. I am also grateful to Martin Albrecht, who co-chaired a Special Session on Lattice-Based Cryptography Constructions and Architectures, and to the contributing authors, Nina Bindel, Tim Güneysu, Tobias Oder, Francesco Regazzoni, Peter Campbell, and Michael Groves.

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 and to the H2020 SAFEcrypto project ([www.safecrypto.eu](http://www.safecrypto.eu)) for providing sponsorship. I appreciate the assistance by Anna Kramer, Abier El-Saeidi and Xavier Mathew from Springer in the production of the proceedings. Finally, I am incredibly thankful to conference officer (general chair) Lizzi Lake and her colleagues at the Institute of Mathematics and its Applications for handling all the practical matters of the conference.

December 2017

Máire O’Neill

<http://www.springer.com/978-3-319-71044-0>

Cryptography and Coding

16th IMA International Conference, IMACC 2017, Oxford,

UK, December 12-14, 2017, Proceedings

O'Neill, M. (Ed.)

2017, X, 393 p. 23 illus., Softcover

ISBN: 978-3-319-71044-0