

## Preface

The International Conference of 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 15th edition was held December 15–17, 2015, in inspirational and historical surroundings at St. Catherine’s College at the University of Oxford.

We received 36 submissions from authors all over the world on a diverse set of topics both in cryptography and coding theory. The Program Committee selected 18 of the submissions for presentation at the conference. The review process was double-blind and rigorous: Each submission was reviewed independently by at least three 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.

The Program Committee selected one distinguished article for the best paper award. Congratulations to Kenneth G. Paterson, Jacob C.N. Schuldt, Dale L. Sibborn, and Hoeteck Wee for winning the award this year with their paper “Security Against Related Randomness Attacks via Reconstructive Extractors.”

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 Sihem Mesnager, Allison Bishop, Alexander May, and Daniel Wichs for accepting our invitation and sharing the insights gathered from their exciting research. Sihem Mesnager kindly offered a companion paper to her talk, “On Existence (Based on an Arithmetical Problem) and Constructions of Bent Functions,” co-authored by Gérard Cohen and David Madore.

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 and Shai Halevi for their cooperation and for letting us use the WebSubRev software to manage the submission and review process. I appreciate the assistance by Alfred Hofmann and Anna Kramer 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 2015

Jens Groth

Cryptography and Coding

15th IMA International Conference, IMACC 2015, Oxford,

UK, December 15-17, 2015. Proceedings

Groth, J. (Ed.)

2015, X, 329 p. 42 illus. in color., Softcover

ISBN: 978-3-319-27238-2