Preface

The 8th International Conference on the Theory and Application of Cryptographic Techniques in Africa, Africacrypt 2016, took place April 13–15, 2016, in Fès, Morocco. The conference was organized by Al Akhawayn University in Ifrane, in cooperation with the International Association for Cryptologic Research (IACR).

The conference received 65 submissions, all of which were reviewed by the Program Committee. Each paper was assigned at least three reviewers, while submissions co-authored by Program Committee members were reviewed by at least four reviewers.

The Program Committee was helped by reports from 48 external reviewers. After highly interactive discussions and a careful deliberation, the Program Committee selected 18 papers for presentation (less than 28 % acceptance rate). The program was completed with invited talks: "Computing on Encrypted Data" by Vinod Vaikuntanathan from MIT and "A New Methodology of Constructing Functional Encryption" by Tatsuaki Okamoto from NTT. We are very grateful to them for accepting our invitation.

We would like to thank everyone who contributed to the success of Africacrypt 2016. We are deeply grateful to the Program Committee for their hard work, enthusiasm, and conscientious efforts to ensure that each paper received a thorough and fair review. These thanks are of course extended to the external reviewers, listed on the following pages, who took the time to help during the evaluation process. We would also like to thank Thomas Baignères and Matthieu Finiasz for writing the iChair software and Springer for agreeing to an accelerated schedule for printing the proceedings.

Our thanks also go to the local Organizing Committee for their commitment and hard work, in order to make the conference an enjoyable experience. They also go to Driss Ouaouicha, President of Al Akhawayn University, and Dean Kevin Smith for their unconditional support. We are deeply grateful to the sponsors Microsoft, Al Akhawayn University, HPS Morocco, the Région Fès-Meknès, ENS, Paris, France, and the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013 Grant Agreement no. 339563 – CryptoCloud), for financially supporting the conference.

Last but not least, we wish to thank the participants, submitters, authors, presenters, and invited speakers, and Program Committees who over the past seven editions have made Africacrypt a highly recognized forum in which researchers can interact and share their work and knowledge with others, for the overall growth and development of cryptology research in the world, and Africa in particular.

April 2016

David Pointcheval
Abderrahmane Nitaj
Tajjeedine Rachidi

http://www.springer.com/978-3-319-31516-4

Progress in Cryptology – AFRICACRYPT 2016
8th International Conference on Cryptology in Africa,
Fes, Morocco, April 13-15, 2016, Proceedings
Pointcheval, D.; Nitaj, A.; Rachidi, T. (Eds.)
2016, X, 369 p. 49 illus., Softcover
ISBN: 978-3-319-31516-4