

# Preface

Latincrypt 2015, the 4th International Conference on Cryptology and Information Security in Latin America, took place August 23–26, 2015, in Guadalajara, Mexico. The main conference program was preceded by the Advanced School on Cryptology and Information Security in Latin America (ASCrypto) August 22–23, 2015. Latincrypt 2015 was organized by the Computer Science Department of CINVESTAV-IPN, in cooperation with The International Association for Cryptologic Research (IACR). The general chairs of the conference were Luis J. Dominguez Perez and Francisco Rodríguez-Henríquez.

The conference received 59 submissions, of which 10 were withdrawn under various circumstances, mainly at the authors' request. Each submission was assigned to at least three committee members. Submissions co-authored by members of the Program Committee were assigned to at least five committee members. The reviewing process was challenging owing to the large number of high-quality submissions, and we are deeply grateful to the committee members and external reviewers for their indefatigable work. Special thanks go out to the shepherds of this edition, who greatly helped us in making a better paper selection. Particularly, we would like to thank Paulo Barreto, Jérémie Detrey, Sorina Ionica, and Gregory Neven, for their outstanding reviewer activities.

After careful deliberation, the Program Committee, which was chaired by Kristin Lauter and Francisco Rodríguez-Henríquez, selected 20 submissions for presentation at the conference. In addition to these presentations, the program also included one session of talks by graduate students and four invited talks by Yuriy Bulygin and Andrew Furtak (Intel, USA), Jung Hee Cheon (Seoul National University, South Korea), Tal Rabin (Thomas J. Watson Research Center, USA), and Adi Shamir (Weizmann Institute, Israel).

The reviewing process was run using the WebSubRev software, written by Shai Halevi from IBM Research. We are grateful to him for releasing this software. Finally, we would like to thank our sponsors, namely, Intel Guadalajara, Microsoft Research, and Oracle for their financial support as well as all the people who contributed to the success of this conference. We are also indebted to the members of the Latincrypt Steering Committee and the general chairs for their diligent work and for making this conference possible. We would also like to thank Springer for accepting to publish the proceedings in the *Lecture Notes in Computer Science* series. It was a great honor to be Program Committee chairs for Latincrypt 2015 and we look forward to the next edition in the conference series.

August 2015

Kristin Lauter  
Francisco Rodríguez-Henríquez

Progress in Cryptology -- LATINCRYPT 2015  
4th International Conference on Cryptology and  
Information Security in Latin America, Guadalajara,  
Mexico, August 23-26, 2015, Proceedings  
Lauter, K.; Rodríguez-Henríquez, F. (Eds.)  
2015, XII, 385 p. 35 illus., Softcover  
ISBN: 978-3-319-22173-1