

Preface

Latincrypt 2014 was the Third International Conference on Cryptology and Information Security in Latin America and took place during September 17–19, 2014 in Florianópolis, Brazil. Latincrypt 2014 was organized by the Computer Security Laboratory (LabSEC) – Universidade Federal de Santa Catarina, in cooperation with The International Association for Cryptologic Research (IACR). The General Chairs of the conference were Ricardo Custódio and Daniel Panario.

The conference received 48 submissions, of which 5 were withdrawn under various circumstances (authors' request, being identified, randomly generated, or already published in another venue). 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 due to the large number of high-quality submissions, and we are deeply grateful to the committee members and external reviewers for their outstanding work. After careful deliberation, the Program Committee, which was chaired by Diego F. Aranha and Alfred Menezes, selected 19 submissions for presentation at the conference. In addition to these presentations, the program also included two sessions of talks by graduate students and four invited talks by Jacob Appelbaum, Claudia Diaz, J. Alex Halderman, and Kristin Lauter. The articles in this volume include the accepted submissions and an invited paper corresponding to Kristin Lauter's invited talk.

The reviewing process was run using the WebSubRev software, written by Shai Halevi from IBM Research and hosted on the IACR server. We are grateful to him for setting up the reviewing website and providing invaluable support during the entire process.

Finally, we would like to thank our sponsors CAPES, CNPq, FAPESC, CGI.br, and NIC.br for their financial support as well as all the people who contributed to the success of this conference. In particular, we are 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 has been a great honor to be PC chairs for Latincrypt 2014 and we look forward to the next edition in the conference series.

October 2014

Diego F. Aranha
Alfred Menezes

Progress in Cryptology - LATINCRYPT 2014
Third International Conference on Cryptology and
Information Security in Latin America Florianópolis,
Brazil, September 17-19, 2014 Revised Selected Papers
Aranha, D.F.; Menezes, A. (Eds.)
2015, XII, 387 p. 64 illus., Softcover
ISBN: 978-3-319-16294-2