

# Preface

This volume contains the papers accepted for presentation at C2SI-Berger2015, in honor of Prof. Thierry Berger, from XLIM Laboratory, University of Limoges, France. C2SI-Berger2015 is an international conference on the theory, and applications of cryptographic techniques, coding theory, and information security. The first aim of this conference is to pay homage to Prof. Thierry Berger for his valuable contribution in teaching and disseminating knowledge in coding theory and cryptography in Morocco since 2003. The second aim of the conference is to provide an international forum for researchers from academia and practitioners from industry, from all over the world for discussion of all forms of cryptography, coding theory, and information security.

The initiative of organizing C2SI-Berger2015 has been started by the Moroccan Laboratory of Mathematics, Computing sciences and Applications (LabMiA) at Faculty of Sciences of the University Mohammed V in Rabat and performed by an active team of researchers from Morocco and France. The conference was organized in cooperation with the International Association for Cryptologic Research (IACR), and the proceedings were published in Springer's Lecture Notes in Computer Science series.

The C2SI-Berger2015 Program Committee consisted of 39 members. There were 59 papers submitted to the conference. Each paper was assigned to at least two members of the Program Committee and was refereed anonymously. The review process was challenging and the Program Committee, aided by reports from 17 external reviewers, produced a total of 130 reviews in all. After this period, 22 papers were accepted on March 20, 2015. Authors then had the opportunity to update their papers until March 25, 2015. The present proceedings include all the revised papers. We are indebted to the members of the Program Committee and the external reviewers for their diligent work.

The conference was honored by the presence of the invited speakers François Arnault, Ezedin Barka, Johannes A. Buchmann, Anne Canteaut, Claude Carlet, Jean Louis Lanet, Ayoub Otmani, and Felix Ulmer. They gave talks on various topics in cryptography, coding theory, and information security and contributed to the success of the conference.

We had the privilege to chair the Program Committee. We would like to thank all committee members for their work on the submissions, as well as all external reviewers for their support. We thank the invited speakers, and the authors of all submissions. They all contributed to the success of the conference.

We would also like to thank Prof. Saaid Amzazi, President of University Mohammed V in Rabat and Prof. Wail Benjelloun, former Head of University Mohammed V, Agdal in Rabat for their unwavering support to research and teaching in the areas of cryptography, coding theory, and information security.

We are deeply grateful to Prof. Thierry Berger and his laboratory XLIM of the University of Limoges for great services in contributing to the establishment of a successful master's degree in coding theory, cryptography, and information security at

University Mohammed V in Rabat. We would like to take this opportunity to acknowledge their professional work.

Finally, we heartily thank all the Local Organizing Committee members, all sponsors, and everyone who contributed to the success of this conference. We are also thankful to the staff at Springer for their help in producing the proceedings.

May 2015

Said El Hajji  
Abderrahmane Nitaj  
El Mamoun Souidi

Codes, Cryptology, and Information Security  
First International Conference, C2SI 2015, Rabat,  
Morocco, May 26-28, 2015, Proceedings - In Honor of  
Thierry Berger  
El Hajji, S.; Nitaj, A.; Carlet, C.; Souidi, E.M. (Eds.)  
2015, XXVI, 375 p. 58 illus., Softcover  
ISBN: 978-3-319-18680-1