Preface

This volume contains the papers accepted for presentation at C2SI-Carlet 2017, in honor of Professor Claude Carlet, from the University of Paris 8, France. C2SI-Carlet is an international conference on the theory and applications of cryptographic techniques, coding theory, and information security. One aim of this conference is to pay homage to Claude Carlet for his valuable contribution in teaching and disseminating knowledge in coding theory and cryptography worldwide, especially in Africa. The other 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 cryptology, coding theory, and information security.

The initiative of organizing C2SI-Carlet 2017 was initiated by the Moroccan Laboratory of Mathematics, Computing Sciences and Applications (LabMIA) at the Faculty of Sciences of the Mohammed V University 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 are published in Springer's *Lecture Notes in Computer Science* series.

The first conference in this series was held at the same university during May 26–28, 2015, for which the proceedings were published in Springer's *Lecture Notes in Computer Sciences* as volume 9084.

The C2SI-Carlet 2017 Program Committee consisted of 49 members. There were 72 papers submitted to the conference. Each paper was assigned to two or three members of the Program Committee and was reviewed anonymously. The review process was challenging and the Program Committee, aided by reports from 26 external reviewers, produced a total of 164 reviews in all. After this period, 19 papers were accepted on January 28, 2017. Authors then had the opportunity to update their papers until February 6, 2017. 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 Mohammed Essaaidi, Caroline Fontaine, Maria Isabel Garcia Planas, Sylvain Guilley, and Tor Helleseth. 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 authors of all submissions and all the speakers as well all the participants. They all contributed to the success of the conference.

We also would like to thank Professor Saaid Amzazi, Head of Mohammed V University in Rabat, for his unwavering support to research and teaching in the areas of cryptography, coding theory, and information security. We also want to thank Professor Mourad El Belkacemi, Dean of Faculty of Sciences in Rabat.

We are deeply grateful to Professor Claude Carlet for the great service in contributing to the establishment of a successful research group in coding theory, cryptography, and information security at the Faculty of Sciences of Mohammed V University in Rabat. We would like to take this opportunity to acknowledge his professional work.

Along with these individuals, we wish to thank our local colleagues and students who contributed greatly to the organization and success of the conference.

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 with producing the proceedings and to the staff of EasyChair for the use of their conference management system.

April 2017   S. El Hajji
                                                                         A. Nitaj
                                                                      E.M. Souidi