

Special issue of selected papers of 17th Central European Conference on Cryptology

Preface

This volume contains a set of selected papers submitted for 17-th Central European Conference in Cryptology that was held in Warsaw Technical University in Poland, 4-6 July 2017. It was inaugurated in 2000 at the 14th Czech and Slovak International Conference on Number Theory in Liptovski Jan, Slovak Republic, with a special crypto session and since then has been organized in a selected Central European country every year. The aim of the CECC is to gather people involved in cryptology. The talks cover a wide range of topics including symmetric or asymmetric algorithms and protocols, as well as practical and theoretical aspects of computer security and computational number theory. This edition gathered over 50 persons from Europe and all the world. 11 articles related to applied cryptography were published in the *Int. J. Electronics and Telecom.* v. 64 n. 2, (2018) and nine more theoretical papers were submitted for the special conference volume of *Fundamenta Informaticae*. They were then subjected to a 3 round review process by the journal experts. Ultimately, 5 papers were selected to be published in this special conference volume. The issues of these works include the following topics: encryptions, hashing, randomness, curves and compression. We wish to express our deep appreciation to the authors for their contributions and to the reviewers for their careful, insightful and constructive reviews.

July, 2019

Special issue editors:

Mieczysław Kula

University of Silesia in Katowice, Poland

kula@ux2.math.us.edu.pl

Damian Niwiński

University of Warsaw, Poland

niwinski@mimuw.edu.pl

Jacek Pomykała

University of Warsaw, Poland

pomykala@mimuw.edu.pl