

Preface

This volume contains the papers presented at BalkanCryptSec 2015, the Second International Conference on Cryptography and Information Security in the Balkans, held September 3–4, 2015, in Koper, Slovenia.

The call for papers was answered by 27 submissions from 15 countries. Each submission was reviewed by at least three Program Committee members. After the conference a second round of reviews was held for the revised papers. The committee decided to select 12 papers for the proceedings.

The Program Committee consisted of 28 members representing 18 countries. These members were carefully selected to represent academia and industry, as well as to include world-class experts in various research fields of interest to BalkanCryptSec.

Additionally, the workshop included three excellent invited talks and a tutorial talk. Kaisa Nyberg from Aalto University, Finland, talked about multidimensional linear attacks in a presentation entitled “Key-Variance in Statistical Cryptanalysis.” Alexander Pott from Otto-von-Guericke University of Magdeburg discussed his research in a talk entitled “Almost Perfect Nonlinear and Planar Functions: A Survey of (not so) Recent Results and Open Problems.” Billy Bob Brumley from Tampere University of Technology presented results, techniques, and the evolution of certain attack methods in “Software-Based Side-Channel Attacks.” Enes Pasalic also held a tutorial talk titled “Constructing Boolean Functions for Stream Ciphers.”

We would like to thank everyone who made the conference possible. First and foremost the authors who submitted their papers, in particular the authors of the accepted papers, and the invited speakers. The hard task of reading, commenting, debating, and finally selecting the papers for the conference fell on the Program Committee members. The Program Committee also used two external reviewers, whom we wish to thank as well.

We would also like to thank the local Organizing Committee and especially Nastja Cepak, a PhD student in cryptography at University of Primorska, for her enormous help in arranging and taking care of most of the tasks related to this conference.

This was the second annual BalkanCryptSec conference. The first one was held in 2014 thanks to Svetla Nikova and Tsonka Baicheva’s idea of hosting a cryptography and security conference in the Balkans. We hope and believe the conference will continue for many years to come.

November 2015

Enes Pasalic
Lars R. Knudsen

Cryptography and Information Security in the Balkans
Second International Conference, BalkanCryptSec
2015, Koper, Slovenia, September 3-4, 2015, Revised
Selected Papers

Pasalic, E.; Knudsen, L.R. (Eds.)

2016, VIII, 207 p. 19 illus., Softcover

ISBN: 978-3-319-29171-0