

Preface

This year was marked by the fifth edition of the International Workshop on Lightweight Cryptography for Security and Privacy (LightSec). With the increasing deployment of ubiquitous systems and pervasive computing, the field of low-resource cryptography is becoming more relevant and timely than ever. Following the series of four previous events held in Turkey and Germany, LightSec 2016 was organized during September 20–21, 2016, at Aksaray University in Cappadocia, Turkey. This volume contains the papers presented at the workshop.

There were 18 submissions from ten countries. Each submission was reviewed by at least three, and on average 3.5, Program Committee members in a careful double-blind review process stretched over a month. Having performed a total of 63 reviews with the help of 11 external reviewers, after an active discussion phase, the committee decided to accept nine papers. The Program Committee consisted of 20 top-notch researchers in the field of lightweight security from ten countries.

LightSec 2016 featured two invited talks. On the first day, based on her unique mix of academic and industrial backgrounds, Elif Bilge Kavun from Infineon, Germany, gave an insightful lecture on “Resource-Efficient Cryptography: Addressing the Gaps in Lightweight Solutions.” On the second day, Orhun Kara from TUBITAK BILGEM, representing the government sector, gave an excellent talk on “Block Ciphers vs. Stream Ciphers on Ultra Lightweight Platforms” covering the recent trends in stream cipher design.

We would like to express our gratitude to all the Program Committee members and external reviewers for their exemplary review work that resulted in selecting the high-quality papers that constitute this volume. We thank all authors for submitting their work to LightSec 2016. We would also like to thank both invited speakers for their invaluable contributions to the workshop. Special thanks go to Atilla Elçi, who served as the general chair of the workshop and whose organization was outstanding. We are indebted to the Aksaray University, Faculty of Engineering, Department of Electrical-Electronics Engineering, for hosting the event. The workshop would have been unthinkable without the constant support and astute advice of the Steering Committee in general as well as of Orhun Kara and Ali Aydin Selcuk in particular. We are also obliged to the International Association for Cryptologic Research for deciding to grant LightSec 2016 the “In Cooperation with IACR” status.

December 2016

Andrey Bogdanov

Lightweight Cryptography for Security and Privacy
5th International Workshop, LightSec 2016, Aksaray,
Turkey, September 21-22, 2016, Revised Selected
Papers
Bogdanov, A. (Ed.)
2017, VII, 149 p. 34 illus., Softcover
ISBN: 978-3-319-55713-7