

Preface

The International Workshop on Lightweight Cryptography for Security and Privacy (LightSec) was established to promote novel research on the security and privacy issues for applications that can be termed as lightweight security due to the associated constraints on metrics such as available power, energy, computing ability, area, execution time, and memory requirements. While such applications are becoming ubiquitous in daily life, they are also affecting a greater portion of society, leading to a plethora of economic-, security- and privacy-related concerns. The first three editions of LightSec took place in Turkey. This fourth edition of LightSec was held in Germany and was organized by the Horst Görtz Institute for IT Security (HGI) at Ruhr University Bochum (RUB). The workshop had 53 participants from 12 different countries. LightSec 2015 received generous financial support by the Ruhr University Bochum, the graduate school Ubicrypt, and eurobits.

LightSec received 17 submissions that underwent a review process. Each paper was reviewed by three reviewers. The entire double-blinded review process took more than two months in which the merits and weaknesses of each paper were carefully taken into account. The Program Committee finally accepted 10 original articles that were presented at the workshop and published in these proceedings.

LightSec featured four invited talks. On the first day Christian Rechberger from the Technical University Denmark and Miroslav Knezevic from NXP Semiconductor gave excellent lectures on “Lightweight Crypto on a Full Circle: From Industry to Academia and Back” and “Designing Crypto for Low Energy and Low Power,” respectively. The second day featured invited talks by Roberto Avanzi from QUALCOMM on “What the Industry Really Needs” in the area of lightweight crypto, and by Meltem Sömez Turan from the National Institute of Standards and Technology (NIST) about the NIST initiative on lightweight cryptography.

We thank all the Program Committee members and external reviewers for their invaluable contribution to the selection process. Their technical comments and insights ensured the quality of the selected papers in these proceedings. Of course, we would also like to thank the authors for submitting their original research papers to LightSec 2015. We are very much indebted to our four invited speakers for their extremely interesting and entertaining presentations.

Last but not least, the successful organization of the event would not have been possible without the great reliable help of Irmgard Kühn, who took care of all the big and small issues that arose. Finally, we hope that these proceedings are as interesting to read as it was to compile them. We are already looking forward to the next editions of LightSec, wherever they take place.

November 2015

Tim Güneysu
Gregor Leander
Amir Moradi

Lightweight Cryptography for Security and Privacy
4th International Workshop, LightSec 2015, Bochum,
Germany, September 10-11, 2015, Revised Selected
Papers

Güneysu, T.; Leander, G.; Moradi, A. (Eds.)
2016, IX, 165 p. 44 illus. in color., Softcover
ISBN: 978-3-319-29077-5