

Preface

LightSec 2014 is the Third International Workshop on Lightweight Cryptography for Security and Privacy, which was held in Eminönü, Istanbul, Turkey, during September 1–2, 2014. The workshop was sponsored by TÜBİTAK BİLGEM UEKAE (The Scientific and Technological Research Council of Turkey, National Research Institute of Electronics and Cryptology) and held in cooperation with the International Association of Cryptologic Research (IACR).

The Program Committee (PC) consisted of 31 members representing 13 countries. There were 24 papers from 15 countries submitted to the workshop. Submitted papers were reviewed by the PC members themselves or by assigned subreviewers. Each submission was double-blind reviewed by at least three PC members and the submissions by PC members were assigned to 14 subreviewers. The vast majority of the papers were reviewed by four reviewers. Twelve of the papers were accepted for presentation at the workshop, whereas two of them were conditionally accepted. These two conditionally accepted papers were later withdrawn.

The program also included three excellent invited talks by experts in the field. The first talk was given by Tolga Acar from Microsoft Research titled “Selecting and Deploying Elliptic Curves in Security Protocols.” The second talk was given by Guido Marco Bertoni from ST Microelectronics titled “Permutation-based encryption for lightweight applications.” The final invited talk was delivered by Johann Heyszl from Fraunhofer AISEC titled “High-Resolution Magnetic Field Side-Channels and their Affect on Cryptographic Implementations.”

We would like to thank all the people and organizations who contributed to making the workshop successful. First, we greatly appreciate the valuable work of the authors and we thank them for submitting their manuscripts to LightSec 2014. We are also grateful to the PC members and the External Reviewers whose admirable effort in reviewing the submissions definitely enhanced the scientific quality of the program. Thanks also to the invited speakers, Tolga Acar, Guido Marco Bertoni, and Johann Heyszl, for their willingness to participate in LightSec 2014. We would like to also thank Istanbul Chamber of Commerce and Istanbul Commerce University, who made this workshop possible by letting us use their facilities. We would like to thank Ali Boyacı and Serhan Yarkan from EE Engineering Department at Istanbul Commerce University for their admirable help in organizing the workshop. Last but not least, we would like to thank students of the EE Engineering Department at Istanbul Commerce University, for their help in running the workshop.

September 2014

Erdinç Öztürk
Thomas Eisenbarth

Lightweight Cryptography for Security and Privacy
Third International Workshop, LightSec 2014, Istanbul,
Turkey, September 1-2, 2014, Revised Selected Papers
Eisenbarth, Th.; Öztürk, E. (Eds.)
2015, XIII, 169 p. 33 illus., Softcover
ISBN: 978-3-319-16362-8