Preface

The 22nd International Workshop on Fast Software Encryption (FSE 2015) was held in Istanbul, Turkey, March 8–11, 2015. The workshop was organized by TUBITAK - BILGEM with Hüseyin Demirci serving as the general chair and sponsored by the International Association for Cryptologic Research (IACR). The workshop had about 140 registered participants from 26 different countries.

FSE 2015 received 71 valid submissions. Each paper was reviewed by three reviewers and five reviewers in the case of a submission co-authored by members of the Program Committee. The entire double-blind review process took more than two months in which each paper was carefully taken into account. The Program Committee finally accepted 28 original articles to be presented at the workshop and published in these proceedings.

The Program Committee of FSE 2015 decided, in line with the tradition of previous years, to select a best paper. This year, the Program Committee awarded the contribution "GCM Security Bounds Reconsidered" by Yuichi Niwa, Keisuke Ohashi, Kazuhiko Minematsu, and Tetsu Iwata the best paper award of FSE 2015. This paper, along with the two contributions "Rotational Cryptanalysis of ARX Revisited" by Dmitry Khovratovich, Ivica Nikolić, Josef Pieprzyk, Przemysław Sokołowski, and Ron Steinfeld and "Meet-in-the-Middle Attacks and Structural Analysis of Round-Reduced PRINCE" by Patrick Derbezand and Léo Perrin, was furthermore solicited for the *Journal of Cryptology*.

FSE 2015 featured two invited talks, one by Meltem Sönmez Turan from the National Institute of Standards and Technology (NIST) about the NIST initiative on lightweight cryptography, and one by Jacob Appelbaum on NSA, mass surveillance, and its impact on society. The program of FSE 2015 also included a rump session with short talks on the latest results in the field. The rump session was chaired by Dan Bernstein and Tanja Lange.

The selection of papers would not have been possible without the enormous help of the Program Committee members and external reviewers. I am grateful for all their effort. It was great honor and good fun to work together with such an excellent committee.

For the local organization, I would like to express my gratitude to Hüseyin Demirci for the very professional and smooth organization of the workshop. Without him and his team, the event would not have been possible.

Finally, I hope that the reader enjoys these proceedings as much as I enjoyed the experiences of serving as program chair for FSE 2015.

May 2015 Gregor Leander

http://www.springer.com/978-3-662-48115-8

Fast Software Encryption
22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers
Leander, G. (Ed.)
2015, XI, 600 p. 131 illus., Softcover
ISBN: 978-3-662-48115-8