Preface

The 10th International Workshop on Security (IWSEC 2015) was held at Todaiji Cultural Center, in Nara, Japan, during August 26-28, 2015. The workshop was organized by CSEC of IPSJ (Special Interest Group on Computer Security of Information Processing Society of Japan) and supported by ISEC in ESS of IEICE (Technical Committee on Information and Communication Engineers).

This year, the workshop received 58 submissions. Finally, 18 papers were accepted as regular papers, and 3 papers were accepted as short papers. Each submission was anonymously reviewed by at least four reviewers, and these proceedings contain the revised versions of the accepted papers. In addition to the presentations of the papers, the workshop also featured a poster session.

The best paper award was given to "Identity-based Lossy Encryption from Learning with Errors" by Jingnan He, Bao Li, Xianhui Lu, Dingding Jia, Haiyang Xue, and Xiaochao Sun, and the best student paper award was given to "Improved (Pseudo) Preimage Attacks on Reduced-Round GOST and Grøstl-256 and Studies on Several Truncation Patterns for AES-like Compression Functions" by Bingke Ma, Bao Li, Ronglin Hao, and Xiaoqian Li.

A number of people contributed to the success of IWSEC 2015. We would like to thank the authors for submitting their papers to the workshop. The selection of the papers was a challenging and dedicated task, and we are deeply grateful to the members of Program Committee and the external reviewers for their in-depth reviews and detailed discussions. We are also grateful to Andrei Voronkov for developing EasyChair, which was used for the paper submission, reviews, discussions, and preparation of these proceedings.

Last but not least, we would like to thank the general co-chairs, Yukiyasu Tsunoo and Satoru Torii, for leading the Local Organizing Committee, and we also would like to thank the members of the Local Organizing Committee for their efforts to ensure the smooth running of the workshop.

June 2015

Keisuke Tanaka
Yuji Suga



http://www.springer.com/978-3-319-22424-4

Advances in Information and Computer Security
10th International Workshop on Security, IWSEC 2015,
Nara, Japan, August 26-28, 2015, Proceedings
Tanaka, K.; Suga, Y. (Eds.)
2015, XIII, 357 p. 51 illus., Softcover
ISBN: 978-3-319-22424-4