

Preface

ASIACRYPT 2016, the 22nd Annual International Conference on Theory and Application of Cryptology and Information Security, was held at InterContinental Hanoi Westlake Hotel in Hanoi, Vietnam, during December 4–8, 2016. The conference focused on all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

Asiacrypt 2016 received a total of 240 submissions from all over the world. The Program Committee selected 67 papers from these submissions for publication in the proceedings of this conference. The review process was made via the usual double-blind peer review by the Program Committee comprising 43 leading experts in the field. Each submission was reviewed by at least three reviewers and five reviewers were assigned to submissions co-authored by Program Committee members. This year, the conference operated a two-round review system with a rebuttal phase. In the first-round review the Program Committee selected the 140 submissions that were considered of value for proceeding to the second round. In the second-round review the Program Committee further reviewed the submissions by taking into account their rebuttal letter from the authors. The selection process was assisted by a total of 309 external reviewers. These two-volume proceedings contain the revised versions of the papers that were selected. The revised versions were not reviewed again and the authors are responsible for their contents.

The program of Asiacrypt 2016 featured three excellent invited talks. Nadia Heninger gave a talk on “The Reality of Cryptographic Deployments on the Internet,” Hoeteck Wee spoke on “Advances in Functional Encryption,” and Neal Koblitz gave a non-technical lecture on “Cryptography in Vietnam in the French and American Wars.” The conference also featured a traditional rump session that contained short presentations on the latest research results of the field. The Program Committee selected the work “Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds” by Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène for the Best Paper Award of Asiacrypt 2016. Two more papers, “Nonlinear Invariant Attack—Practical Attack on Full SCREAM, iSCREAM, and Midori64” by Yosuke Todo, Gregor Leander, Yu Sasaki and “Ciphertext Clipping: Clipping the Power of Kleptographic Attacks” by Alexander Russell, Qiang Tang, Moti Yung, Hong-Sheng Zhou were solicited to submit full versions to the *Journal of Cryptology*.

Many people contributed to the success of Asiacrypt 2016. We would like to thank the authors for submitting their research results to the conference. We are very grateful to all of the Program Committee members as well as the external reviewers for their fruitful comments and discussions on their areas of expertise. We are greatly indebted to Ngo Bao Chau and Phan Duong Hieu, the general co-chairs for their efforts and overall organization. We would also like to thank Nguyen Huu Du, Nguyen Quoc Khanh, Nguyen Duy Lan, Duong Ngoc Thai, Nguyen Ta Toan Khoa, Nguyen Ngoc Tuan,

Le Thi Lan Anh, and the local Organizing Committee for their continuous supports. We thank Steven Galbraith for expertly organizing and chairing the rump session.

Finally we thank Shai Halevi for letting us use his nice software for supporting the paper submission and review process. We also thank Alfred Hofmann, Anna Kramer, and their colleagues at Springer for handling the editorial process of the proceedings. We would like to express our gratitude to our partners and sponsors: XLIM, Microsoft Research, CISCO, Intel, Google.

December 2016

Jung Hee Cheon
Tsuyoshi Takagi



<http://www.springer.com/978-3-662-53889-0>

Advances in Cryptology - ASIACRYPT 2016
22nd International Conference on the Theory and
Application of Cryptology and Information Security,
Hanoi, Vietnam, December 4-8, 2016, Proceedings,
Part II

Cheon, J.H.; Takagi, T. (Eds.)

2016, XXIV, 1055 p. 198 illus., Softcover

ISBN: 978-3-662-53889-0