# Preface

CRYPTO 2015, the 35th Annual International Cryptology Conference, was held August 16–20, 2015, on the campus of the University of California, Santa Barbara. The event was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the UCSB Computer Science Department.

The program of CRYPTO 2015 reflects significant advances and trends in all areas of cryptology. Seventy-four papers were included in the program; this two-volume proceedings contains the revised versions of these papers. The program also included two invited talks: Shai Halevi on 'The state of cryptographic multilinear maps' and Ed Felten on 'Cryptography, Security, and Public Safety: A Policy Perspective'. The paper "Integral Cryptanalysis on Full MISTY1" by Yosuke Todo was selected for both the best paper award and the award for the best paper authored by a young researcher.

This year we received a record number of submissions (266), and in an effort to accommodate as many high-quality submissions as possible, the conference ran in two parallel sessions.

The papers were reviewed by a Program Committee (PC) consisting of 40 leading researchers in the field, in addition to the two co-chairs. Each PC member was allowed to submit two papers. Papers were reviewed in a double-blind fashion, with each paper assigned to three reviewers (four for PC-authored papers). During the discussion phase, when necessary, extra reviews were solicited.

We would like to sincerely thank the authors of all submissions—those whose papers made it into the program and those whose papers did not. Our deep appreciation also goes out to the PC members, who invested an extraordinary amount of time in reviewing papers, and to the many external reviewers who significantly contributed to the comprehensive evaluation of the submissions. A list of PC members and external reviewers follows. Despite all our efforts, the list of external reviewers may contain errors or omissions; we apologize for that in advance.

We would like to thank Tom Ristenpart, the general chair, for working closely with us throughout the whole process and providing the much-needed support at every step, including artfully creating and maintaining the website and taking care of all aspects of the conference's logistics—particularly the novel double-track arrangements.

As always, special thanks are due to Shai Halevi for providing his tireless support of the *websubrev* software, which we used for the whole conference planning and operation, including paper submission and evaluation, interaction among PC members, and communication with the authors. Alfred Hofmann and his colleagues at Springer provided a meticulous service for the timely production of this volume.

Finally, we would like to thank Qualcomm, NSF, and Microsoft for sponsoring the conference, and Cryptography Research for their continuous support.

August 2015

Rosario Gennaro
Matthew Robshaw