Preface

Eurocrypt 2016, the 35th annual International Conference on the Theory and Applications of Cryptographic Techniques, was held in Vienna, Austria, during May 8–12, 2016. The conference was sponsored by the International Association for Cryptologic Research (IACR). Krzysztof Pietrzak (IST Austria), together with Joël Alwen, Georg Fuchsbauer, Peter Gaži (all IST Austria), and Eike Kiltz (Ruhr-Universität Bochum), were responsible for the local organization. They were supported by a local organizing team consisting of Hamza Abusalah, Chethan Kamath, and Michal Rybár (all IST Austria). We are indebted to them for their support and smooth collaboration.

The conference program followed the now established parallel track system where the works of the authors were presented in two concurrently running tracks. As in the previous edition of Eurocrypt, one track was labeled $\mathcal{R}$ (for real) and the other one was labeled $\mathcal{I}$ (for ideal). Only the invited talks, the tutorial, the best paper, papers with honorable mentions, and the final session of the conference spanned over both tracks.

The proceedings of Eurocrypt contain 62 papers selected from 274 submissions, which corresponds to a record number of submissions in the history of Eurocrypt. Each submission was anonymized for the reviewing process and was assigned to at least three of the 55 Program Committee members. Submissions co-authored by committee members were assigned to at least four members. Committee members were allowed to submit at most one paper, or two if both were co-authored. The reviewing process included a first-round notification followed by a rebuttal for papers that made it to the second round. After extensive deliberations the Program Committee accepted 62 papers. The revised versions of these papers are included in these two-volume proceedings.

The committee decided to give the Best Paper Award to "Tightly Secure CCA-Secure Encryption Without Pairings" by Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. The two runners-up to the award, "Indistinguishability Obfuscation from Constant-Degree Graded Encoding Schemes" by Huijia Lin and "Essentially Optimal Robust Secret Sharing with Maximal Corruptions" by Allison Bishop, Valerio Pastro, Rajmohan Rajaraman, Daniel and Wichs, received honorable mentions. All three papers received invitations for the *Journal of Cryptology*.

The program also included invited talks by Karthikeyan Bhargavan, entitled "Protecting Transport Layer Security from Legacy Vulnerabilities", Bart Preneel, entitled "The Future of Cryptography" (IACR distinguished lecture), and Christian Collberg, entitled "Engineering Code Obfuscation." In addition, Emmanuel Prouff gave a tutorial about "Securing Cryptography Implementations in Embedded Systems." All the speakers were so kind as to also provide a short abstract for the proceedings.

We would like to thank all the authors who submitted papers. We know that the Program Committee's decisions, especially rejections of very good papers that did not find a slot among the sparse number of accepted papers, can be very disappointing. We sincerely hope that the rejected works eventually get the attention they deserve.

We are also indebted to the Program Committee members and all external reviewers for their voluntary work, especially since the newly established and unified page limits and the increasing number of submissions induce quite a workload. It has been an honor to work with everyone. The committee's work was tremendously simplified by Shai Halevi's submission software and his support, including running the service on IACR servers.

Finally, we thank everyone else—speakers, session chairs, and rump session chairs—for their contribution to the program of Eurocrypt 2016.

May 2016

Marc Fischlin
Jean-Sébastien Coron

http://www.springer.com/978-3-662-49889-7

Advances in Cryptology – EUROCRYPT 2016
35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I
Fischlin, M.; Coron, J.-S. (Eds.)
2016, XXVIII, 853 p. 155 illus., Softcover
ISBN: 978-3-662-49889-7