Preface

The 20th International Workshop on Fast Software Encryption (FSE 2013) was held at Novotel Singapore Clarke Quay, Singapore, during March 11–13, 2013. The workshop was sponsored by the International Association for Cryptologic Research. FSE 2013 received 97 submissions from 24 countries. The 21 members of the Program Committee were assisted by more than 90 external reviewers. In total, they delivered 337 reviews. Each submission was reviewed by at least three Program Committee members. Submissions by Program Committee members received at least five reviews. The review process was double-blind, and conflicts of interest were carefully handled. The review process was handled through an online review system that supported discussions among Program Committee members. Over the entire review period, more than 200 messages were exchanged between Program Committee members. Eventually, the Program Committee selected 30 papers (a 31 % acceptance rate) for publication in the proceedings.

The program also included two invited talks, by Serge Vaudenay from Ecole Polytechnique Federale de Lausanne, Switzerland, and by Daniel Bernstein from University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, The Netherlands.

The Program Committee also identified the best submissions from FSE for their scientific quality, their originality, and their clarity. The FSE 2013 Best Paper Award went to Gordon Procter and Carlos Cid from Royal Holloway, University of London, United Kingdom. Their paper, "On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes", identifies some properties of hash functions based on polynomial evaluation that arise from the underlying algebraic structure.

Many people contributed to FSE 2013. We thank the authors for contributing their excellent research. We thank the Program Committee members, and their external reviewers, for making a significant effort to select for the program. We particularly thank Dmitry Khovratovich, Subhamoy Maitra, Florian Mendel, and Christian Rechberger for shepherding papers. Finally, we thank Jian Guo and Thomas Peyrin, the general co-chairs, and the FSE Steering Committee members, who worked so hard for the event and helped me a lot.

FSE 2013 collected a diversity of recent results in symmetric cryptography, from theory to practical aspects, from design to cryptanalysis. We feel privileged for the opportunity to develop the FSE 2013 program. We hope that the papers in these proceedings will continue to inspire, guide, and clarify your academic and professional endeavors.

May 2014   Shiho Moriai

Springer