Preface

The 21st International Workshop on Fast Software Encryption (FSE 2014) was held in London March 3–5, 2014. The workshop was organized in cooperation with the International Association for Cryptologic Research, and took place at London's Natural History Museum. The workshop had 156 registered participants, of which 31 were students.

The FSE 2014 Program Committee comprised 26 members, and counted on the support of 75 external reviewers. We received 99 valid submissions, and each submission was reviewed by at least three PC members. After more than two months of deliberation and discussions, a total of 31 papers were accepted. This has been the highest number of accepted papers for an FSE so far, driven by the rather high quality of submissions. We are very grateful to all PC members and reviewers for their effort and contribution to the selection of an outstanding program of original articles in symmetric cryptography.

Besides the 31 selected talks, the workshop program also included two invited talks: Thomas Johansson from Lund University spoke on the application of low weight polynomials in cryptography; Thomas Ristenpart from the University of Wisconsin-Madison closed the workshop with the talk "New Encryption Primitives for Uncertain Times." The workshop also featured a rump session, chaired by Dan Bernstein and Tanja Lange, with several short informal presentations.

As it is tradition, the FSE 2014 Program Committee was asked to select the best submissions to the workshop, based on their scientific quality and contribution. Two submissions received the award for best papers: "Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes" by Daniel Augot and Matthieu Finiasz, and "Differential-Linear Cryptanalysis Revisited" by Céline Blondeau, Gregor Leander, and Kaisa Nyberg. The two papers also received a special solicitation for submission to the *Journal of Cryptology*.

In addition to the authors, PC members, and external reviewers, several other people contributed to the success of FSE 2014: colleagues, students, and supporting staff at DTU and Royal Holloway (in particular Claire Hudson); Shai Halevi, Greg Rose and abhi shelat at the IACR; the members of the FSE Steering Committee; Anne Kramer at Springer; and staff at the Natural History Museum. We were also fortunate to count on the financial support of four sponsors (CESG, KPMG, NXP, and Visa Europe), which made it possible to hold the event in such an impressive venue. We are very grateful to you all for your support.

It was a great honor to have been in charge of the organization of FSE 2014 and to coordinate the selection of its scientific program. It gave us the opportunity to work with a number of outstanding researchers and professionals in the cryptographic community; we were very pleased with its success and greatly enjoyed it. We hope the reader also enjoys the papers in these proceedings.

January 2015

Carlos Cid
Christian Rechberger

http://www.springer.com/978-3-662-46705-3

Fast Software Encryption
21st International Workshop, FSE 2014, London, UK,
March 3-5, 2014. Revised Selected Papers
Cid, C.; Rechberger, C. (Eds.)
2015, XI, 636 p. 155 illus., Softcover
ISBN: 978-3-662-46705-3