

# Preface

The Fast Software Encryption Workshop 1999 is the sixth in a series of workshops starting in Cambridge in December 1993.

The workshop was organized by General Chair William Wolfowicz, Fondazione U. Bordoni, and Programme Chair Lars Knudsen, University of Bergen, Norway, in cooperation with Securteam, as far as local arrangements were concerned. The workshop was held March 24-26, 1999 in Rome, Italy.

The workshop concentrated on all aspects of fast secret key ciphers, including the design and cryptanalysis of block and stream ciphers, as well as hash functions.

There were 51 submissions, all of them submitted electronically. One submission was later withdrawn by the authors, and 22 papers were selected for presentation. All submissions were carefully reviewed by at least 4 committee members. At the workshop, preliminary versions of all 22 papers were distributed to all attendees. After the workshop there was a final reviewing process with additional comments to the authors.

It has been a challenge for me to chair the committee of this workshop, and it is a pleasure to thank all the members of the programme committee for their hard work. The committee this year consisted of, in alphabetic order, Ross Anderson (Cambridge, UK), Eli Biham (Technion, Israel), Don Coppersmith (IBM, USA), Cunsheng Ding (Singapore), Dieter Gollmann (Microsoft, UK), James Massey (Denmark), Mitsuru Matsui (Mitsubishi, Japan), Bart Preneel (K.U. Leuven, Belgium), Bruce Schneier (Counterpane, USA), and Serge Vaudenay (ENS, France).

It is a great pleasure to thank William Wolfowicz for organising the workshop. Also, it is a pleasure to thank Securteam for the logistics and Telsy and Sun for supporting the conference. Finally, a big thank you to all submitting authors for their contributions, and to all attendees (approximately 165) of the workshop. Finally, I would like to thank Vincent Rijmen for his technical assistance in preparing these proceedings.

April 1999

Lars Knudsen

Fast Software Encryption

6th International Workshop, FSE'99 Rome, Italy, March

24-26, 1999 Proceedings

Knudsen, L. (Ed.)

1999, VIII, 324 p., Softcover

ISBN: 978-3-540-66226-6