Fast Software Encryption Workshop 1997 (FSE4)
CALL FOR PAPERS

January 20-22, 1997, Haifa, Israel
NOTE CHANGE OF DATES

The first Fast Software Encryption workshop was held in Cambridge in December 1993, and followed by two workshops in Leuven in December 1994, and in Cambridge in February 1996. The workshop concentrates on all aspects of fast ciphers, including the design and cryptanalysis of block and stream ciphers, as well as hash functions. The fourth Fast Software Encryption workshop will be held from January 20 to January 22, 1997, in Haifa, Israel. The workshop is organized by the Technion, in co-operation with the International Association for Cryptologic Research.

Instructions for Authors

Interested parties are invited to submit original unpublished papers on the design and analysis of fast encryption algorithms and hash functions. It is strongly preferred that the papers be processed in LaTeX using llncs.sty, and not exceed 15 pages in length. The LaTeX files are to be sent electronically, together with the email and smail addresses of the sender. If papers are submitted in paper form, eight copies are required. The papers should not be submitted simultaneously to other workshops or conferences with proceedings.

Conference Proceedings

Preproceedings will be available at the meeting. The final proceedings is expected to be published in the Springer-Verlag Lecture Notes in Computer Science.

Addresses for submission

biham@cs.technion.ac.il
Eli Biham, Computer Science Department, Technion, Haifa 32000, Israel

For more information

This call for papers and other information are available at the world wide web at URL: `http://www.cs.technion.ac.il/~biham/Fse4/`. For more information, contact the addresses above.

Important Dates

Paper submission:	October 11, 1996
Notification of acceptance:	November 24, 1996
Final copy for the preproceedings:	December 19, 1996
The workshop:	January 20-22, 1997
Final copy for the proceedings:	February 20, 1997

Program Committee

Eli Biham (Technion - chair), Ross Anderson (Cambridge University), Don Coppersmith (IBM Research), Cunsheng Ding (Turku), Dieter Gollmann (Royal Holloway), Jim Massey (ETH Zurich), Mitsuru Matsui (Mitsubishi), Bart Preneel (Katholieke Universiteit Leuven).