Fast Software Encryption Workshop 2002

CALL FOR PAPERS

February 4-6, 2002, Leuven, Belgium

The Fast Software Encryption workshop has been held 8 times, the first one in Cambridge December 1993, and the latest in Yokohama April 2001. The workshop concentrates on all aspects of fast symmetric primitives: secret key ciphers, including the design and cryptanalysis of block and stream ciphers, as well as hash functions and message authentication codes (MACs). The ninth Fast Software Encryption workshop will be held in February 2002 in Leuven, Belgium. The workshop is organized by Matt Landrock (General Chair), Joan Daemen and Vincent Rijmen (Program Co-chairs).

Instructions for Authors
Interested parties are invited to submit original unpublished papers on the design and analysis of fast encryption algorithms and hash functions. The papers must not be submitted simultaneously to other workshops or conferences with proceedings. The submissions must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It is strongly preferred that submissions be processed in LaTeX according to http://www.springer.de/comp/lncs/authors.html since this will be a mandatory requirement for the final papers. The paper must not exceed 15 pages in length. The papers are to be sent electronically in LaTeX, PostScript or Portable Document Format (PDF), together with the email and physical addresses of the sender. Preproceedings will be available at the meeting and the final proceedings will be published in the Springer-Verlag Lecture Notes in Computer Science. Notification of acceptance or rejection will be sent to authors by January 1, 2002. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Address for Submission: FSE-Submission@protonworld.com

Important Dates

Paper submission:	November 15, 2001
Notification of acceptance:	January 1, 2002
Final copy for preproceedings:	January 20, 2002
The workshop:	February 4-6, 2002
Final copy for the proceedings:	March 31, 2002

Program Committee:

Vincent Rijmen (co-chair, Katholieke Universiteit Leuven)
Joan Daemen (co-chair, ProtonWorld Int'l)
Ross Anderson (Cambridge University)
Eli Biham (Technion)
Don Coppersmith (IBM)
Cunsheng Ding (Hong Kong University of Science and Technology)
Thomas Johansson (Lund University)
Mitsuru Matsui (Mitsubishi Electric)
Willi Meier (Fachhochschule Aargau)
Kaisa Nyberg (Nokia)
Bart Preneel (Katholieke Universiteit Leuven)

Further Information

Further information will be made available on the conference web site: http://www.cryptomathic.com/fse2002.