FSE 2003

February 24-26, 2003
Lund, Sweden

Call for Papers

Original research papers on technical aspects of symmetric cryptology are invited for submission to Fast Software Encryption workshop 2003. The workshop concentrates on all aspects of fast primitives for symmetric cryptography: secret key ciphers, the design and cryptanalysis of block and stream ciphers, as well as hash functions and message authentication codes (MACs).

FSE 2003 is the tenth annual FSE workshop, for the second year sponsored by the International Association for Cryptologic Research (IACR), and organized in cooperation with the Department of Information Technology, Lund University. Important dates are:

Conference	February 24 - 26, 2003
Submission deadline	November 30, 2002
Notification of decision	January 15, 2003
Pre-proceedings version deadline	February 10, 2003
Proceedings version deadline	March 30, 2003

Instructions for Authors

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other international conference or workshop.

Submission Format: The submission must be anonymous, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The length of the submission should be at most 12 pages excluding bibliography and appendices. It should use at least 11-point fonts and have reasonable sized margins. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Committee members are not required to read appendices; the paper should be intelligible without them. Submissions not meeting these guidelines risk rejection without consideration of their merits. It is strongly preferred that submissions be processed in LaTeX according to the instructions listed on www.springer.de/comp/lncs/authors.html, since this will be a mandatory requirement for the final papers.

Submission: Submitted papers must be in PDF (www.fastlane.nsf.gov/a1/pdfcreat.htm) or postscript format and should be submitted electronically to fse2003@it.lth.se. In the email body should be included name and address of all authors as well as an email address to the corresponding author. **Submission deadline: November 30, 2002.**

Decisions and Presentation: Notification of acceptance or rejection will be sent to authors by January 15, 2003. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Conference Proceedings: Pre-proceedings will be available at the workshop. Final proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science. Instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers.

Program Committee

Ross Anderson	Cambridge University, UK
Anne Canteaut	Inria, France
Joan Daemen	Protonworld, Belgium
Cunsheng Ding	Hong Kong University of Science and Technology
Hans Dobbertin	University of Bochum, Germany
Henri Gilbert	France Telecom, France
Jovan Golic	Gemplus, Italy
Thomas Johansson (chair)	Lund University, Sweden
Lars Knudsen	Technical University of Denmark
Helger Lipmaa	Helsinki University of Technology, Finland
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	Fachhochschule Aargau, Switzerland
Kaisa Nyberg	Nokia, Finland
Bart Preneel	K.U. Leuven, Belgium
Vincent Rijmen	Cryptomathic, Belgium
Matt Robshaw	Royal Holloway, University of London, UK
Serge Vaudenay	EPFL, Switzerland
David Wagner	U.C. Berkeley, USA

Workshop information

Further information is available on the FSE 2003 webpage **www.it.lth.se/fse03**. For other information, contact: Ben Smeets (general chair), Ericsson Mobile Platforms, Lund, Sweden, email: fse2003_org@it.lth.se

Stipends: A limited number of stipends are available to those unable to obtain funding to attend the conference. Students whose papers are accepted and who will present the paper themselves are encouraged to apply if such assistance is needed. Requests for stipends should be addressed to the General Chair.