Fast Software Encryption—FSE 2006

March 15-17, 2006

Graz, Austria

http://fse2006.iaik.tugraz.at/

Call for Papers

FSE 2006 is the 13th annual Fast Software Encryption workshop, for the fifth year sponsored by the International Association for Cryptologic Research (IACR). Original research papers on symmetric cryptology are invited for submission to FSE 2006. The workshop concentrates on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, analysis and evaluation tools, hash functions, and message authentication codes (MACs).

Important Dates

Submission deadline	November 25, 2005
Notification of decision	January 27, 2006
Pre-proceedings version deadline	February 24, 2006
Workshop	March 15-17, 2006
Proceedings version deadline	April 7, 2006

Instructions for Authors

Submissions must not substantially duplicate work that has been published elsewhere or submitted in parallel to any journal or conference or workshop with proceedings. IACR reserves the right to share information about submissions with other Program Committees to detect parallel submissions. 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 have reasonably sized margins and fonts (at least 10pt). 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 http://www.springer.de/comp/lncs/authors.html since these are mandatory for the final papers. Submitted papers must be in PDF or postscript format and submitted electronically. A description of the submission procedure is available via `http://fse2006.iaik.tugraz.at/`. Authors of accepted papers must guarantee that their paper will be presented at the workshop.

Proceedings

Pre-proceedings will be available at the workshop. Proceedings are intended to be published in Springer-Verlag's Lecture Notes in Computer Science series. Authors of accepted papers will be required to complete the IACR copyright assignment form at `http://www.iacr.org/forms/copyright_agreement.html` for their work to be published in the workshop proceedings.

Program Committee

Kazumaro Aoki	NTT, Japan
Steve Babbage	Vodafone, U.K.
Anne Canteaut	INRIA, France
Carlos Cid	Royal Holloway, University of London, U.K.
Joan Daemen	STMicroelectronics, Belgium
Orr Dunkelman	Technion - Israel Institute of Technology, Israel
Helena Handschuh	Spansion, France
Thomas Johansson	Lund University, Sweden
Antoine Joux	DGA + University of Versailles, France
Charanjit Jutla	IBM Watson, U.S.A.
Xuejia Lai	Shanghai Jiaotong University, China
Stefan Lucks	University of Mannheim, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FH Aargau, Switzerland
Kaisa Nyberg	Helsinki University of Technology + Nokia, Finland
Elisabeth Oswald	Graz University of Technology, Austria
Bart Preneel	K.U.Leuven, Belgium
Håvard Raddum	University of Bergen, Norway
Matt Robshaw (chair)	France Telecom R&D, France
Phillip Rogaway	U.C.Davis, U.S.A. + Mah Fah Luang Univ., Thailand
Moti Yung	Columbia University, U.S.A.

Workshop Information and Stipends

The primary source of information is `http://fse2006.iaik.tugraz.at/` but any remaining questions can be sent to `info-fse2006@iaik.tugraz.at`. A limited number of stipends are available to those unable to obtain funding to attend the workshop. 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 sent to `info-fse2006@iaik.tugraz.at`.