FSE 2010
Call for Papers

February 7–10, Seoul, Korea
http://cist.korea.ac.kr/~fse2010/

Submission deadline November 9, 2009 (23:59:59 UTC)
Notification of decision January 6, 2010
Pre-proceedings version deadline January 26, 2010
Workshop February 7–10, 2010
Proceedings version deadline March 31, 2010

General Information

FSE 2010 is the 17th annual Fast Software Encryption workshop, for the ninth year sponsored by the International Association for Cryptologic Research (IACR). FSE 2010 will take place in Seoul, Korea. Original research papers on symmetric cryptology are invited for submission to FSE 2010. 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).

Instructions for Authors

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/is planning to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings. IACR reserves the right to share information about submissions with other program committees to detect parallel submissions and the IACR policy on irregular submissions will be strictly enforced. See http://www.iacr.org/irregular.html for further details.

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 14 pages excluding bibliography and appendices using single column with at least 11pt size font, reasonably sized margins and in total not more than 20 pages. 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 format and should be submitted electronically. A detailed description of the electronic submission procedure will be available via http://cist.korea.ac.kr/~fse2010/.

The authors of submitted papers guarantee that their paper will be presented at the workshop if their paper is accepted.

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.
Workshop Information and Stipends

The primary source of information is http://cist.korea.ac.kr/~fse2010/. 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 fse2010@cist.korea.ac.kr.

Program Committee

Daniel J. Bernstein  
University of Illinois at Chicago, USA

Alex Biryukov  
University of Luxembourg, Luxembourg

Joan Daemen  
STMicroelectronics, Belgium

Orr Dunkelman  
École normale supérieure, France, and Weizmann Institute, Israel

Helena Handschuh  
Katholieke Universiteit Leuven, Belgium

Thomas Johansson  
Lund University, Sweden

Antoine Joux  
DGA and Université de Versailles, France

Charanjit S. Jutla  
IBM T. J. Watson Research Center, USA

Stefan Lucks  
Bauhaus-University Weimar, Germany

Mitsuru Matsui  
Mitsubishi Electric, Japan

Willi Meier  
FHNW, Switzerland

Kaisa Nyberg  
Helsinki University of Technology and NOKIA, Finland

Elisabeth Oswald  
University of Bristol, UK

Josef Pieprzyk  
Macquarie University, Australia

Bart Preneel  
Katholieke Universiteit Leuven, Belgium

Christian Rechberger  
IAIK, Graz University of Technology, Austria

Thomas Ristenpart  
UC San Diego, USA

Matt Robshaw  
Orange Labs, France

Palash Sarkar  
Indian Statistical Institute, India

Serge Vaudenay  
EPFL, Switzerland

Kan Yasuda  
NTT, Japan

Program co-Chairs

Seokhie Hong  
Korea University, Korea

Tetsu Iwata  
Nagoya University, Japan

General co-Chairs

Jongin Lim  
Korea University, Korea

Jongsung Kim  
Kyungnam University, Korea

Contact Information

All correspondence and/or questions should be directed to either of the following organizational committee members:

Seokhie Hong  
Program co-Chair  
CIST, Korea University  
Anam Dong, Sungbuk Gu, Seoul, Korea  
Email: fse2010@cse.nagoya-u.ac.jp

Tetsu Iwata  
Program co-Chair  
Dept. of Computational Sci. and Eng.,  
Nagoya University  
Furo-cho, Chikusa-ku, Nagoya, 464-8603, Japan  
Email: fse2010@cse.nagoya-u.ac.jp

Jongin Lim  
General co-Chair  
CIST, Korea University  
Anam Dong, Sungbuk Gu, Seoul, Korea  
Email: fse2010@cist.korea.ac.kr

Jongsung Kim  
General co-Chair  
Division of e-Business, Kyungnam University  
449 Wolyeong-dong, Masan, Kyungnam, Korea  
Email: fse2010@cist.korea.ac.kr