

ECRYPT Workshop on Cryptographic Hash Functions

May 24–25, 2007

Barcelona, Spain

<http://events.iaik.tugraz.at/HashWorkshop07/>

Call for Papers

In view of the rapid developments in the cryptanalysis and design of cryptographic hash functions, the symmetric crypto lab (STVL) of ECRYPT organizes a dedicated workshop. The workshop will take place right after Eurocrypt 2007. The aim of the workshop is to attract researchers and application developers both from academia and industry. We encourage presentations and reports on preliminary work that the participants plan to publish later elsewhere. Topics for submission include, but are not limited to:

- Cryptanalysis of hash functions
- Design of new hash functions, compression functions and structures
- Desirable properties for hash functions
- Relation between applications and security properties of hash functions

We also welcome non-research oriented input from industry, e.g. about the functional and security requirements in applications.

Important dates

Submission deadline	March 31, 2007
Notification of decision	April 26, 2007
Final version deadline	May 10, 2007
Workshop	May 24–25, 2007

Instructions for Authors

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. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader.

Submitted papers must be in PDF or postscript format and should be submitted electronically. Detailed description of the electronic submission procedure is available at the conference web site. Authors of accepted papers must guarantee that their paper will be presented at the workshop.

Proceedings

There will be no formal proceedings. Accepted papers and presentations will be posted on the workshop website and included in a workshop handout.

Program Committee

Anne Canteaut	INRIA, France
Carlos Cid	Royal Holloway, University of London, U.K.
Joan Daemen	STMicroelectronics, Belgium
Orr Dunkelman	K.U.Leuven, Belgium
Praveen Gauravaram	Queensland University of Technology, Australia
Thomas Johansson	Lund University, Sweden
Bart Preneel	K.U.Leuven, Belgium
Vincent Rijmen (chair)	Graz University of Technology, Austria
Matt Robshaw	France Telecom R&D, France

Organizing Committee

Jordi Herrera-Joancomart	Florian Mendel, Norbert Pramstaller, Christian Rechberger, Vincent Rijmen, Michaela Tretter
Universitat Oberta de Catalunya, Spain	Graz University of Technology, Austria

Stipends

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 addressed to the program chair.