ASIACRYPT 2010

December 5-9, 2010 — Singapore

Call for Papers

Original research papers on all technical aspects of cryptology are solicited for submission to ASIACRYPT 2010, the annual International Conference on Theory and Application of Cryptology and Information Security. The conference is sponsored by the International Association for Cryptologic Research (IACR) in cooperation with Nanyang Technological University (NTU). The conference homepage is
`http://www.spms.ntu.edu.sg/asiacrypt2010/index.html`.

Important Dates:

Submission Deadline:	May 20, 2010 23:59:59 UTC
Notifications to Authors:	August 17, 2010
Proceedings Version Deadline:	September 10, 2010
ASIACRYPT 2010 Conference:	December 5-9, 2010

Instructions for Authors:

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to a journal or any other conference/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. For further details, see
`http://www.iacr.org/irregular.html`.

The submission must be anonymous with no author names, affiliations or obvious references. The length of the submission must be at most 16 pages excluding references and appendices. The text should be in a single column format, in at least 11-point fonts and have reasonable margins. The length of the final versions for Springer's LNCS will be at most 18 pages including everything. The submission should begin with a title, a short abstract and a list of keywords. The introduction should summarize the contributions of the paper at the level understandable for a non-expert reader. The reviewers 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 encouraged that submission be processed in LaTeX2ε. Authors should refer to the instructions listed on
`http://www.springer.de/comp/lncs/authors.html`
for typesetting their manuscripts. These instructions 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 announced at the conference homepage.

The proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science series and available at the conference. Authors of accepted papers must complete the IACR copyright assignment form at
`http://www.iacr.org/forms/copyright_agreement.html`
for their work to be published in the proceedings, and guarantee that their paper will be presented at the conference.

Stipend:

Students whose papers have been accepted and who present their talk at the conference will have their registration waived. A limited number of stipends is available to those unable to obtain funding to attend the conference. Students presenting their papers will be given preference. Requests for registration waiver and/or stipends should be addressed to General Chair.

General Chair:

San Ling
Nanyang Technological University, Singapore
Tel: +65 6513 8468
Email: ac2010-general@ntu.edu.sg

Program Chair:

Masayuki Abe
NTT Information Sharing Platform Laboratories, Japan
Tel: +81 422 59 3631
Email: ac2010-pc-chair@ntu.edu.sg

Program Committee Members:

Claude Carlet	University of Paris 8, France
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Yevgeniy Dodis	New York University, USA
Marc Fischlin	Darmstadt University of Technology, Germany
Henri Gilbert	France Telecom, France
Dennis Hofheinz	Karlsruhe Institute of Technology, Germany
Thomas Johansson	Lund University, Sweden
Antoine Joux	DGA and Université de Versailles, PRISM, France
Jonathan Katz	University of Maryland, USA
Lars R. Knudsen	Technical University of Denmark, Denmark
Kaoru Kurosawa	Ibaraki University, Japan
Xuejia Lai	Shanghai Jiao Tong University, China
Dong Hoon Lee	Korea University, Korea
Anna Lysyanskaya	Brown University, USA
Vadim Lyubashevsky	Tel Aviv University, Israel
Mitsuru Matsui	Mitsubishi Electric, Japan
Payman Mohassel	University of Calgary, Canada
Phong Q. Nguyen	INRIA and ENS, France
Jesper Buus Nielsen	Aarhus University, Denmark
Kaisa Nyberg	Helsinki University of Technology, Finland
Elisabeth Oswald	University of Bristol, UK
Renato Renner	ETH Zurich, Switzerland
Vincent Rijmen	K. U. Leuven, Belgium and TU Graz, Austria
Thomas Shrimpton	Portland State University, USA
Nigel P. Smart	University of Bristol, UK
François-Xavier Standaert	UCL, Belgium
Ron Steinfeld	Macquarie University, Australia
Willy Susilo	University of Wollongong, Australia
Vinod Vaikuntanathan	IBM Research, USA
Serge Vaudenay	EPFL, Switzerland
Hoeteck Wee	Queens College, CUNY, USA
Hongjun Wu	Institute for Infocomm Research, Singapore
Kan Yasuda	NTT, Japan
Hong-Sheng Zhou	University of Connecticut, USA