ASIACRYPT 2007

December 2-6, 2007, Kuching, Sarawak, MALAYSIA

Call for Papers

Original research papers on all technical aspects of cryptology are solicited for submission to ASIACRYPT 2007, 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 the Information Security Research (iSECURES) Lab of Swinburne University of Technology (Sarawak Campus) and the Sarawak Development Institute (SDI); and financially supported by the Sarawak Government. See www.swinburne.edu.my/asiacrypt2007. Important dates are:

Submission deadline	Decision notification	Proceedings version	Conference
June 1 (21:00 GMT), 2007	August 15, 2007	September 7, 2007	December 2 - 6, 2007

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, 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 should be **at most 12 pages excluding bibliography and appendices**. It should be in single column format, use at least 11-point fonts, and have reasonable margins.
- 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 a level appropriate for a non-specialist reader. Committee members are not required to read appendices; the paper should be intelligible without them.
- Submissions should preferably be in PDF format (i.e., a .pdf file) although PostScript (i.e., a .ps file) will be allowed. (The submission server will be available in late April 2007.)

Conference Proceedings: Proceedings will be published in Springer's *Lecture Notes in Computer Science*, and will be available at the conference.

Visas: It is strongly recommended that authors (from countries requiring visa) apply for visa at the time of submission. Do not wait for the notification decisions. (Contact the General Chair for more information.)

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.

Program Committee

Masayuki Abe (NTT)
Alex Biryukov (University of Luxembourg)
Alexandra Boldyreva (Georgia Institute of Technology)
Jung Hee Cheon (Seoul National University)
Jean-Sebastien Coron (University of Luxembourg)
Joan Daemen (STMicroelectronics)
Serge Fehr (CWI)
Steven Galbraith (Royal Holloway Univ. of London)
Craig Gentry (Stanford University)
Henri Gilbert (France Telecom)
Shai Halevi (IBM T.J. Watson Research Center)
Helena Handschuh (Spansion)
Tetsu Iwata (Nagoya University)
Thomas Johansson (Lund University)
Marc Joye (Thomson R&D France)
Jonathan Katz (University of Maryland)
Lars R. Knudsen (Technical University of Denmark)
Hugo Krawczyk (IBM T.J. Watson Research Center)
Kaoru Kurosawa (Ibaraki University), chair
Xuejia Lai (Shanghai Jiaotong University)
Arjen K. Lenstra (EPFL IC LACAL)
Stefan Lucks (Bauhaus-University Weimar)
Anna Lysyanskaya (Brown University)
Alexander May (Technische Universität Darmstadt)
Jesper Buus Nielsen (University of Aarhus)
Elisabeth Oswald (University of Bristol)
Bart Preneel (Katholieke Universiteit Leuven)
Pandu Rangan (Indian Institute of Technology)
Nigel Smart (University Bristol)
Palash Sarkar (Indian Statistical Institute)
Tsuyoshi Takagi (Future University-Hakodate)
Serge Vaudenay (EPFL)
Brent Waters (SRI International)
Stefan Wolf (ETH Zurich)

General Chair: Raphael C.-W. Phan
EPFL - I&C - ISC - LASEC
Station 14 - Building INF
CH-1015 Lausanne
Switzerland
Tel: +41 21 693 8127 Fax: +41 21 693 7689
Email: asiacrypt2007@iacr.org

Program Chair: Kaoru Kurosawa
Dept. of Computer & Information Sciences
Ibaraki University
4-12-1 Nakanarusawa, Hitachi, Ibaraki
316-8511 Japan
Tel/Fax: +81 294 38 5135
Email: ac2007@mx.ibaraki.ac.jp