ASIACRYPT 2000

December 3–7, 2000, Kyoto, JAPAN

Second CALL FOR PAPERS

`http://www.iacr.org/conferences/ac2000`

Original papers on all technical aspects of cryptology are solicited for submission to ASIACRYPT 2000, the Sixth Annual ASIACRYPT Conference. ASIACRYPT 2000 will be held at the Kyoto International Conference Hall Kyoto, Japan, from December 3 to 7, 2000. ASIACRYPT 2000 is organized by the International Association for Cryptologic Research (IACR), in cooperation with IEICE Technical Group on Information Security and IPSJ Computer Security Group.

Instructions for authors: Authors are strongly encouraged to submit their papers electronically. A detailed description of the electronic submission procedure will appear by March 1, 2000 at the ASIACRYPT 2000 web pages. Electronic submissions must conform to this procedure and be received by May 25, 2000, 15:00 JST (6:00am GMT) in order to be considered. Authors unable to submit electronically are invited to send a cover letter and 22 copies of an anonymous paper (double-sided copies preferred) to the Program Chair at the postal address below. Submissions must be received by the Program Chair on or before May 25, 2000 (or postmarked by May 15, 2000, and sent via airmail or courier). Late submissions and submissions by fax will not be considered. The cover letter should contain the paper's title and the names and affiliations of the authors, and should identify the contact author including e-mail and postal addresses.

Submissions must not substantially duplicate work that any of the authors have published elsewhere or have submitted in parallel to any other conference or workshop that has proceedings. The paper 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 key words, and its introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. The paper should be at most 12 pages excluding the bibliography and clearly marked appendices, and at most 20 pages in total, using at least 11 point font and reasonable margins. 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. Notification of acceptance or rejection will be sent to authors by August 5, 2000. Authors of accepted papers must guarantee that their paper will be presented at the conference.

Conference proceedings: Proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science and will be available at the conference. Clear instructions about the preparation of a final proceedings version will be sent to the authors of accepted papers (http://www.springer.de/comp/lncs/authors.html). The final copies of the accepted papers will be due on September 5, 2000.

Submission: May 25, 2000 **Acceptance:** August 5, 2000 **Proceedings version:** September 5, 2000

Program committee:

Ross Anderson (Cambridge University, UK)
Johannes Buchmann (Technical University of Darmstadt, Germany)
Yvo Desmedt (Florida State University, USA)
Ueli Maurer (ETH Zurich, Switzerland)
Moni Naor (Weizmann Institute, Israel)
Choonsik Park (ETRI, Korea)
Phillip Rogaway (University of California at Davis, USA)
Kouichi Sakurai (Kyushu University, Japan)
Serge Vaudenay (EPF Lausanne, Switzerland)
Moti Yung (CertCo, USA)
Dan Boneh (Stanford University, USA)
Ivan Damgård (Arhus University, Denmark)
Yongfei Han (SecurEworld, Singapore)
Alfred Menezes (University of Waterloo, Canada)
Tatsuaki Okamoto, chair (NTT Labs, Japan)
Dingyi Pei (Chinese Academy of Science, China)
Kazue Sako (NEC, Japan)
Jacques Stern (ENS, France)
Chung-Huang Yang (National Kaohsiung First University, Taiwan)
Yuliang Zheng (Monash University, Australia)

Advisory members: Kazumaro Aoki, Electronic submissions (NTT Labs, Japan)
Tsutomu Matsumoto, ASIACRYPT 2000 general chair (Yokohama National University, Japan)
Eiji Okamoto, ASIACRYPT'99 program co-chair (University of Wisconsin, USA)

Address for non-electronic submissions:
Tatsuaki Okamoto
Program Chair, ASIACRYPT 2000
NTT Labs, Room 612A
1-1 Hikarino-oka, Yokosuka-shi
239-0847 Japan
Tel: +81-468-59-2511
Fax: +81-468-59-3858
Email: okamoto@isl.ntt.co.jp

For other information contact:
Tsutomu Matsumoto
General Chair, ASIACRYPT 2000
Yokohama National University,
Division of Artificial Environment and Systems,
79-5 Tokiwadai, Hodogaya-ku, Yokohama
240-8501 Japan,
Tel: +81-45-339-4134
Fax: +81-45-338-1157
Email: tsutomu@mlab.jks.ynu.ac.jp

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.