ASIACRYPT 2012

The 18th Annual International Conference on the Theory and Application of Cryptology and Information Security

December 2 - 6, 2012, Beijing, China

Call for Papers

Original research papers on all technical aspects of cryptology are solicited for submission to ASIACRYPT 2012, the 18th Annual International Conference on Theory and Application of Cryptology and Information Security. The conference is organized by the International Association for Cryptologic Research (IACR) in cooperation with the China Association for Cryptologic Research (CACR) and is supported by National Natural Science Foundation of China (NSFC). The conference homepage is http://cis.sjtu.edu.cn/asiacrypt2012.

Important Dates:

Submission Deadline:	May 20, 2012 23:59:59 UTC
Notifications to Authors:	August 16, 2012
Proceedings Version Deadline:	September 9, 2012
ASIACRYPT 2012 Conference:	December 2-6, 2012

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/docs/irregular.html.

The submission must be anonymous with no author names, affiliations or obvious references. The length of the submission must be at most 14 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 submissions 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 submission server is https://ccs.cs.tsinghua.edu.cn/asiacrypt2012/submit.

The proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science series and will be 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 are 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.

Program Co-chairs:

Xiaoyun Wang
Tsinghua University, China
Tel: +82 10 6279 6671
Email: xiaoyunwang@tsinghua.edu.cn

Kazue Sako
NEC, Japan
Tel: +81 44 431 7686
Email: k-sako@ab.jp.nec.com

General Chair:

Xuejia Lai
Shanghai Jiao Tong University, China
Tel: +86 21 3420 5440
Email: laix@sjtu.edu.cn

Program Committee Members:

Feng Bao	I2R, Singapore
Alex Biryukov	University of Luxembourg, Luxembourg
Xavier Boyen	PARC, USA
David Cash	IBM T.J. Watson Research Center, USA
Jung Hee Cheon	Seoul National University, Korea
Sherman S.M. Chow	University of Waterloo, Canada
Joan Daemen	STMicroelectronics, Belgium
Jintai Ding	University of Cincinnat, USA
Orr Dunkelman	University of Haifa and Weizmann Institute, Israel
Marc Fischlin	Darmstadt University of Technology, Germany
Vipul Goyal	Microsoft Research, India
Tetsu Iwata	Nagoya University, Japan
Antoine Joux	DGA and Universite de Versailles, PRISM, France
Jonathan Katz	University of Maryland, USA
Eike Kiltz	Ruhr University Bochum, Germany
Lars Ramkilde Knudsen	Technical University of Denmark, Denmark
Dong Hoon Lee	Korea University, Korea
Arjen K. Lenstra	EPFL, Switzerland
Dongdai Lin	CAS, China
Mitsuru Matsui	Mitsubishi Electric, Japan
Willi Meier	FHNW, Switzerland
Florian Mendel	Katholieke Universiteit Leuven, Belgium
Phong Q. Nguyen	INRIA, France and Tsinghua University, China
Tatsuaki Okamoto	NTT, Japan
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Christian Rechberger	Technical University of Denmark, Denmark
Rei Safavi-Naini	University of Calgary, Canada
Kazue Sako(PC Co-chairs)	NEC, Japan
Nigel P. Smart	University of Bristol, UK
Ron Steinfeld	Macquarie University, Australia
Xiaoyun Wang (PC Co-chairs)	Tsinghua University, China
Hongjun Wu	Nanyang Technological University, Singapore