ASIACRYPT 2015
Call for Papers

Original research papers on all technical aspects of cryptology are solicited for submission to ASIACRYPT 2015, the 21st Annual International Conference on Theory and Application of Cryptology and Information Security. The conference is organized by the International Association for Cryptologic Research.

Instructions for Authors:

Submissions must be at most 25 pages using the Springer LNCS format, excluding any auxiliary supporting material. Details on the Springer LNCS format can be obtained via `http://www.springer.de/comp/lncs/authors.html`. The final published version of an accepted paper is expected to closely match these 25 pages.

Submissions must be submitted electronically in the PDF format, and the submission procedure and the submission link will be announced at the conference website at a later date. All submissions will be blind-refereed and submissions must be anonymous, with no author names, affiliations, or obvious references. Submissions should begin with a title, a short abstract, and a list of keywords, followed by an introduction, a main body, an appendix (if any), and references, within 25 pages. The introduction should summarize the contributions of the paper at the level understandable for a non-expert reader.

Optionally, if an author desires, a clearly-marked auxiliary supporting material can be appended after the submission. The auxiliary supporting material has no prescribed form or page limit and might be used, for instance, to provide program code or additional experimental data. Alternatively, the auxiliary supporting material can be submitted as a separate file from the submission. The reviewers are not required to read the auxiliary supporting material and submissions should be intelligible without it.

Submissions not meeting these guidelines risk rejection without consideration of their merits. *In particular, the Springer LNCS format must be used without changing margins.*

It is strongly encouraged that submissions be processed in LaTeX. 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.

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/`.

For papers that are accepted, the length of the proceedings version will be at most 25 pages in the Springer LNCS format. 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 available at `http://www.iacr.org/docs/` for their work to be published in the proceedings. Authors of accepted papers must guarantee that their paper will be presented at the conference.

The Program Committee may select a paper for the best paper award.

Important Dates:

- Submission deadline: May 20, 2015, 2:00 a.m. UTC.
- Notification: August 14, 2015.
- Camera-ready version: September 7, 2015.
- Conference: Sunday November 29 to Thursday December 3, 2015.

Stipend:

Students whose papers have been accepted and who present their talks 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 fee waiver and/or stipends should be addressed to the General Chair.

Program Committee:

Daniel J. Bernstein	University of Illinois at Chicago, USA, and Technische Universiteit Eindhoven, The Netherlands
Ignacio Cascudo	Aarhus University, Denmark
Chen-Mou Cheng	National Taiwan University, Taiwan
Sherman S.M. Chow	Chinese University of Hong Kong, Hong Kong
Kai-Min Chung	Academia Sinica, Taiwan
Nico Döttling	Aarhus University, Denmark
Jens Groth	University College London, UK
Dawu Gu	Shanghai Jiaotong University, China
Dong-Guk Han	Kookmin University, Korea
Marc Joye	Technicolor, USA
Nathan Keller	Bar-Ilan University, Israel
Aggelos Kiayias	National and Kapodistrian University of Athens, Greece
Kaoru Kurosawa	Ibaraki University, Japan
Xuejia Lai	Shanghai Jiaotong University, China
Hyang-Sook Lee	Ewha Womans University, Korea
Jooyoung Lee	Sejong University, Korea
Soojoon Lee	Kyung Hee University, Korea
Arjen Lenstra	EPFL, Switzerland
Dongdai Lin	Chinese Academy of Sciences, China
Hemanta K. Maji	UCLA, USA
Alexander May	Ruhr-University Bochum, Germany
Bart Mennink	KU Leuven, Belgium
Tatsuaki Okamoto	NTT, Japan
Raphael C.-W. Phan	Multimedia University, Malaysia
Josef Pieprzyk	Queensland University of Technology, Australia
Bart Preneel	KU Leuven, Belgium
Damien Robert	Inria Bordeaux, France
Giovanni Russello	University of Auckland, New Zealand
Ahmad-Reza Sadeghi	TU Darmstadt, Germany

Rei Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Yu Sasaki	NTT, Japan
Peter Schwabe	Radboud University, The Netherlands
Jae Hong Seo	Myongji University, Korea
Nigel Smart	University of Bristol, UK
Damien Stehlé	ENS de Lyon, France
Tsuyoshi Takagi	Kyushu University, Japan
Mehdi Tibouchi	NTT, Japan
Dominique Unruh	University of Tartu, Estonia
Serge Vaudenay	EPFL, Switzerland
Vesselin Velichkov	University of Luxembourg, Luxembourg
Huaxiong Wang	Nanyang Technological University, Singapore
Hongjun Wu	Nanyang Technological University, Singapore
Vassilis Zikas	ETH Zurich, Switzerland

Contact:

Steven Galbraith — General Chair
University of Auckland, New Zealand
s.galbraith@auckland.ac.nz

Tetsu Iwata — Program Co-chair
Nagoya University, Japan
ac15chair@gmail.com

Jung Hee Cheon — Program Co-chair
Seoul National University, Korea
ac15chair@gmail.com