ASIACRYPT 2009

December 6 - 10, 2009 — Tokyo, Japan

Call for Papers (Version 2.3)

Original research papers on all technical aspects of cryptology are solicited for submission to ASIACRYPT 2009, 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 Technical Group on Information Security (ISEC) of the Institute of Electronics, Information and Communication Engineers (IEICE). The conference homepage is `http://asiacrypt2009.cipher.risk.tsukuba.ac.jp`.

Important Dates

Submission Deadline	May 29, 2009 23:59:59 UTC
Notifications to Authors	August 10, 2009
Proceedings Version Deadline	September 4, 2009
ASIACRYPT 2009 Conference	December 6-10, 2009

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 12 pages excluding references and appendices and at most 18 pages in total. 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 according to the instructions listed on `http://www.springer.de/comp/lncs/authors.html`. 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. Authors unable to submit electronically should contact the program chair by May 1, 2009.

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
Eiji Okamoto
Graduate School of Systems and Information Engineering
University of Tsukuba
1-1-1 Ten-nohdai, Tsukuba, Ibaraki
305-8573 Japan
okamoto@risk.tsukuba.ac.jp

Program Chair
Mitsuru Matsui
Information Technology R&D Labs
Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, Kanagawa
247-8501 Japan
Matsui.Mitsuru@ab.MitsubishiElectric.co.jp

Local Organizing Advisory Committee Members

Hideki Imai	Chuo University	Tsutomu Matsumoto	Yokohama National University
Tatsuaki Okamoto	NTT	Shigeo Tsujii	IISEC

Local Organizing Committee Members

Seigo Arita	IISEC	Eiichiro Fujisaki	NTT
Toru Fujiwara	Osaka University	Keiichi Iwamura	Tokyo University of Science
Akira Kanaoka	University of Tsukuba	Toshinobu Kaneko	Tokyo University of Science
Jun Kogure	Fujitsu Laboratories	Masahiro Mambo	University of Tsukuba
Kanta Matsuura	The University of Tokyo	Natsume Matsuzaki	Panasonic
Atsuko Miyaji	JAIST	Shiho Moriai	Sony
Hirofumi Muratani	Toshiba	Kazuto Ogawa	NHK
Kazuo Ohta	The University of Electro-Communications	Katsuyuki Okeya	Hitachi
Taiichi Saito	Tokyo Denki University	Kouichi Sakurai	Kyushu University
Akashi Satoh	AIST	Tsuyoshi Takagi	Hakodate Future University
Yukiyasu Tsunoo	NEC	Hajime Watanabe	AIST
Atsuhiro Yamagishi	IPA		

Program Committee Members

Masayuki Abe	NTT, Japan
Josh Benaloh	Microsoft Research, US
Daniel J. Bernstein	University of Illinois at Chicago, US
Xavier Boyen	Stanford, US
Claude Carlet	University of Paris 8, France
Kim-Kwang Raymond Choo	Australian Institute of Criminology and Regulatory Institutions Network (RegNet), Australian National University, Australia
Claus Diem	University of Leipzig, Germany
Stefan Dziembowski	University of Rome "La Sapienza", Italy
Serge Fehr	CWI, Netherlands
Jun Furukawa	NEC Corporation, Japan
Henri Gilbert	Orange Labs, France
Jens Groth	University College London, UK
Shai Halevi	IBM, US
Goichiro Hanaoka	AIST, Japan
Helena Handschuh	Katholieke Universiteit Leuven, Belgium
Tetsu Iwata	Nagoya University, Japan
Thomas Johansson	Lund University, Sweden
Marc Joye	Thomson R&D, France
Lars Knudsen	DTU Mathematics, Denmark
Xuejia Lai	Shanghai Jiao Tong University, China
Dong Hoon Lee	Korea University , Korea
Arjen Lenstra	École Polytechnique Fédérale de Lausanne, Switzerland, and Alcatel-Lucent Bell Laboratories, US
Keith Martin	Royal Holloway, University of London, UK
Phong Nguyen	INRIA and ENS, France
Kaisa Nyberg	Helsinki University of Technology and Nokia, Finland
Elisabeth Oswald	University of Bristol, UK
Pascal Paillier	Gemalto Security Labs, France
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	ENS, CNRS and INRIA, France
Manoj Prabhakaran	University of Illinois at Urbana-Champaign, US
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Vincent Rijmen	Katholieke Universiteit Leuven, Belgium and Graz University of Technology, Austria
Phillip Rogaway	University of California, Davis, US
Rei Safavi-Naini	University of Calgary, Canada
Berry Schoenmakers	TU Eindhoven, Netherlands
Francois-Xavier Standaert	Université Catholique de Louvain, Belgium
Serge Vaudenay	École Polytechnique Fédérale de Lausanne, Switzerland
Ivan Visconti	University of Salerno, Italy