PKC '16
19th International Conference
on
Practice and Theory in Public-Key Cryptography

CALL FOR PAPERS

Academia Sinica, Taipei, TAIWAN
March 6-9, 2016

The *International Conference on Practice and Theory in Public-Key Cryptography* (PKC) is organized annually by the International Association for Cryptologic Research (IACR). PKC is IACR's main annual conference focusing specifically on all aspects of Public-Key Cryptography. The PKC'16 proceedings will be published in Springer's LNCS Series and will be available at the conference.

Submissions must not substantially duplicate work that any of the authors has published elsewhere, or has submitted in parallel to any journal or any other conference/workshop with proceedings. Accepted submissions may not appear in any other conference or workshop with proceedings. Submissions violating these rules will be rejected and may entail further consequences. IACR reserves the right to share information about submissions with other program committees to detect parallel submissions.

In order to harmonize submission and publication format, submission text will have the same limit of 30 pages in LNCS format as the final version. This includes title page and references. The submission text can be followed by supplementary material of any length. These rules will be strictly enforced. The paper should be intelligible and self-contained without the supplementary material, as committee members are not required to read them. Submissions should be prepared using LaTeX and submitted as PDF using type-1 fonts. The above guidelines will be strictly enforced. Papers must be submitted electronically; a detailed description of the electronic submission procedure will be provided.

Submissions must be fully anonymous, with no author names, affiliations, acknowledgments, or obvious references. Each paper must start with title, abstract, and keywords, followed by a succinct statement appropriate for a non-specialist reader, specifying the subject addressed, its background, main results, and their significance. Technical details directed to the specialist should then follow.

An author of each accepted paper is required to register and present the paper at the conference.

CONFERENCE CO-CHAIRS

Chen-Mou Cheng
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
doug@ntu.edu.tw

Kai-Min Chung
Institute of Information Science
Academia Sinica
Taipei, Taiwan
kmchung@iis.sinica.edu.tw

PROGRAM CO-CHAIRS

Giuseppe Persiano
Dipartimento di Informatica
Università di Salerno
Salerno, Italy
giuper@gmail.com

Bo-Yin Yang
Academia Sinica
Institute of Information Science
Taipei, Taiwan
byyang@iis.sinica.edu.tw

PROGRAM COMMITTEE

Joel Alwen (IST, Austria)
Paulo Barreto (U. Sao Paulo, Brazil and U. Washington Tacoma, USA)
Carlo Blundo (Università di Salerno, Italy)
Dario Catalano (Università di Catania, Italy)
Melissa Chase (Microsoft Research, USA)
Tung Chou (Technische Universiteit Eindhoven, The Netherlands)
Dana Dachman-Soled (U. of Maryland, USA)
Emiliano De Cristofaro (UCL, UK)
Yvo Desmedt (UT at Dallas, USA, and UCL, UK)
Leo Ducas (CWI, The Netherlands)
Dario Fiore (IMDEA Software Institute, Spain)
Pierre-Alain Fouque (Université Rennes 1, France)
Sanjam Garg (University of California, Berkeley, USA)
Tim Gueneysu (University of Bremen, Germany)
Yuval Ishai (The Technion, Israel and UCLA, USA)
Tanja Lange (TU Eindhoven, The Netherlands)
Benoit Libert (ENS Lyon, France)
Feng-Hao Liu (Florida Atlantic University, USA)
Hemanta Maji (Purdue University, USA)
Alexander May (RU Bochum, Germany)
Phong Q. Nguyen (Inria, France and CNRS/JFLI/University of Tokyo, Japan)
Jesper Buus Nielsen (Aarhus University, Denmark)
Tatsuaki Okamoto (NTT, Japan)
Rafi Ostrovsky (UCLA, USA)
Omkant Pandey (University of California, Berkeley, USA)
Giuseppe Persiano (Università di Salerno, Italy), co-chair
Christophe Petit (University College London, UK)
David Pointcheval (ENS Paris, France)
Ahmad-Reza Sadeghi (TU Darmstadt, Germany)
Dominique Schroeder (Saarland University, CISPA, Germany)
Peter Schwabe (Radboud University, The Netherlands)
Daniel Smith-Tone (NIST, USA)
Damien Stehlé (ENS Lyon, France)
Mehdi Tibouchi (NTT, Japan)
Wen-Guey Tzeng (National Chiao Tung University, Taiwan)
Daniele Venturi (Sapienza University of Rome, Italy)
Bo-Yin Yang (Accademia Sinica, Taiwan), co-chair
Moti Yung (Google and Columbia University, USA)

PUBLICITY CHAIR

Peter Schwabe
Radboud University
The Netherlands
peter@cryptojedi.org

IMPORTANT DATES

Submission of draft paper:	October 6, 2015
Notification of acceptance:	December 11, 2015
Final version due:	January 4, 2016

FURTHER INFORMATION

e-mail: pkc16pcchairs@gmail.com
www: http://troll.iis.sinica.edu.tw/pkc16/