PKC 2020

23rd International Conference on Practice and Theory of Public-Key Cryptography

Edinburgh, Scotland, UK
May 4-7, 2020

https://pkc.iacr.org/2020

Call for Papers

General Chairs

M. Kohlweiss, U. of Edinburgh, UK
P. Wallden, U. of Edinburgh, UK
V. Zikas, U. of Edinburgh, UK

Program Committee Chair

A. Kiayias, U. of Edinburgh, UK

Program Committee Members

G. Alagic, UMD, USA
G. Asharov Bar-Ilan U., Israel
N. Attrapadung AIST, Japan
J. Bos NXP, Germany
C. Bruszka Aalto U., Finland
L. Chen U. Surrey, UK
K.-M. Chung Academia Sinica, Taiwan
D. Dahman-Soled UMD, USA
S. Faust TU Darmstadt, Germany
D. Fiore IMDEA Software Institute, Spain
M. Fischlin Darmstadt U., Germany
G. Fuchsbauer ENS Paris, France
S. Galbraith U. Aukland, New Zealand
J. Gong CNRS and ENS, France
K. Han Seoul National U., South Korea
S. Krenn AIT, Austria
B. Libert CNRS and ENS de Lyon, France
H. Lipmaa Simula UiB, Norway
R. Nishimaki NTT Secure Platform Lab, Japan
M. Okhubo NICT, Japan
E. Orsini KUL, Belgium
O. Pandey Stonybrook U., USA
C. Papamanthou UMD, USA
C. Petit U. Birmingham, UK
T. Prest PQShield Ltd, USA
C. Rafols UPF, Spain
A. Roy U. of Bristol, UK
S. Smardjiska Radboud U., The Netherlands
Y. Song Microsoft Research, Redmond, USA
R. Steinwandt Florida Atlantic U., USA
B. Sunar WPI, USA
A. Takayasu U. of Tokyo, Japan
S. Vaudenay EPFL, Switzerland
D. Venturi U. Roma La Sapienza, Italy
F. Vercauteren KUL, Belgium
C. Xing NTU, Singapore
T. Zacharias of Edinburgh, UK
H.-S. Zhou VCU, USA

Overview

The International Conference on Practice and Theory in Public-Key Cryptography (PKC) is organized annually by the International Association for Cryptologic Research (IACR). It is the main annual conference with an explicit focus on public-key cryptography sponsored by IACR. Original research papers on all aspects of public-key cryptography, covering theory, implementations and applications, are solicited for submission to PKC 2020. Accepted papers will be published by Springer in their Lecture Notes in Computer Science series.

Instructions for authors

Submissions should be prepared using LaTeX and must be in the standard Springer LNCS format, with the (only) modification that page numbers must be displayed -- this can be done by putting \pagestyle{plain} into the preamble. Submissions should begin with a title and a short abstract, followed by an introduction that summarizes the contribution of the paper so that it is understandable to a non-expert in the field. Submissions must be anonymous, with no author names, affiliations, or obvious references. Submissions must be at most 30 pages, including title page, references, and figures. The final published version of an accepted paper is expected to closely match the submitted version. If necessary, clearly marked supplementary material (of unbounded size) may be appended to the actual submission. However, submissions are expected to be intelligible and verifiable without the supplementary material; reviewers are not required to read it. In particular, it is discouraged to move crucial proofs into the supplementary material, and in cases where this is unavoidable it is expected that a short but convincing proof sketch is provided in the main body. Submissions must not substantially duplicate published work or work that has been submitted in parallel to any other journal or conference/workshop with proceedings. All submissions to PKC 2020 are viewed as active submissions throughout the entire review period; they cannot be submitted to any other journal or conference/workshop with proceedings before the notification date. Accepted submissions cannot appear in any other conference or workshop that has proceedings. IACR reserves the right to share information about submissions with other program committees. The IACR Policy on Irregular Submissions and Guidelines for Authors, as well as other resources, are all available via http://www.iacr.org/docs. Papers must be submitted electronically. A detailed description of the electronic submission procedure can be available via the conference web-page https://pkc.iacr.org/2010.

Important dates

Submission: November 2nd, 2019, 09:59:59 UTC
Rebuttal: December 5th, 2019
Author Notification: January 18th, 2020
Camera-Ready: February, 2nd, 2020

PKC Steering Committee

Michel Abdalla (ENS, France), Yvo Desmedt (U. Texas, USA), Goichiro Hanaoka (AIST Japan), Aggelos Kiayias (U. Edinburgh, UK), Dongdai Lin (CAS, China), David Naccache (ENS France), Tatsuaki Okamoto (NTT Labs, Japan), David Pointcheval (ENS France), Kazue Sako (NEC Japan), Moti Yung (Google, USA), Yuliang Zheng (U. Alabama, USA).