The 20th International Conference on the Practice and Theory of Public Key Cryptography

PKC 2017

Amsterdam, The Netherlands | March 28 - 31, 2017

Call for Papers

This is the 20th edition of the *International Conference on Practice and Theory of Public Key Cryptography*, the main annual conference with an explicit focus on public-key cryptography, sponsored by IACR, the *International Association for Cryptologic Research*. Original research papers on all aspects of public-key cryptography, covering theory, implementations and applications, are solicited for submission to PKC 2017. Accepted papers will be published by Springer in their *Lecture Notes in Computer Science* series.

Important Dates

Submission deadline:	October 6, 2016, 19:00 UTC	Proceedings version:	January 10, 2017
Decision notification:	December 15, 2016	Conference:	March 28 - 31, 2017

Program Committee

Masayuki Abe | NTT Secure Platform Labs, Japan
Fabrice Benhamouda | ENS, France & IBM, USA
Nir Bitansky | MIT, USA
Zvika Brakerski | Weizmann Institute, Israel
Nishanth Chandran | Microsoft Research, India
Dana Dachman-Soled | University of Maryland, USA
Nico Döttling | UC Berkeley, USA
Leo Ducas | CWI Amsterdam, Netherlands
Sebastian Faust | Ruhr-University Bochum, Germany
Serge Fehr (chair) | CWI Amsterdam, Netherlands
Dario Fiore | IMDEA Software Institute, Spain
Pierre-Alain Fouque | Rennes 1 University, France
Georg Fuchsbauer | INRIA & ENS, France
Sanjam Garg | UC Berkeley, USA
Jens Groth | University College London, UK
Carmit Hazay | Bar-Ilan University, Israel
Dennis Hofheinz | KIT, Germany
Tibor Jager | Ruhr-University Bochum, Germany
Abhishek Jain | Johns Hopkins University, USA
Marcel Keller | University of Bristol, UK
Markulf Kohlweiss | Microsoft Research, UK
Vadim Lyubashevsky | IBM Zurich, Switzerland
Takahiro Matsuda | AIST, Japan
Adam O'Neill | Georgetown University, USA
Arpita Patra | Indian Institute of Science, India
Ludovic Perret | Sorbonne U., UPMC & INRIA, France
Christophe Petit | University of Oxford, UK
Vanishree Rao | PARC, USA
Gil Segev | Hebrew University of Jerusalem, Israel
Alessandra Scafuro | Boston U. & Northeastern U., USA
Fang Song | University of Waterloo, Canada
Daniele Venturi | University of Trento, Italy
Ivan Visconti | University of Salerno, Italy
Hoeteck Wee | ENS, France
Vassilis Zikas | Rensselaer Polytechnic Institute, USA

Conference Organization

PKC 2017 is organized by *Centrum Wiskunde & Informatica (CWI)* in Amsterdam, the national research institute for mathematics and computer science in the Netherlands.

Program chair:	Serge Fehr | pkc2017programchair@iacr.org
General chair:	Marc Stevens | pkc2017@iacr.org
Advisory member:	Ronald Cramer

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 these submitted pages. 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 2017 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 will be available via the conference web-page `http://www.iacr.org/workshops/pkc2017`. Submissions not meeting any of the guidelines above risk rejection without consideration of their merits. All accepted papers must conform to Springer publishing requirements and authors will be required to sign the IACR *Copyright and Consent Form* when submitting the proceedings version of their papers. Authors must guarantee that their paper, if accepted, will be presented at the conference by one of the authors.

Steering Committee

Ronald Cramer | *CWI & Leiden Univ., Netherlands*
Yvo Desmedt | *University of Texas at Dallas, USA*
Goichiro Hanaoka | *AIST, Japan*
David Naccache | *ENS, France*
Tatsuaki Okamoto | *NTT Labs, Japan*
David Pointcheval | *ENS, France*
Moti Yung | *Google Inc. & Columbia University, USA*
Yuliang Zheng | *Univ. of Alabama at Birmingham, USA*