

# PKC 2015 | Call for Papers

18th International Conference on Practice and Theory in Public-Key Cryptography

March 30–April 1, 2015 | Washington, D.C. (USA)

<http://www.iacr.org/workshops/pkc2015/>



## General Information:

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 the IACR's main annual conference focusing specifically on all aspects of public-key cryptography. In 2015 the conference will be held at the US National Institute of Standards and Technology (NIST), near Washington, D.C. (USA).

Original research papers on all aspects of public-key cryptography—including theory, design, analysis, cryptanalysis, implementation, and applications—are solicited for submission. Papers must not be submitted simultaneously to any journal or another conference with published proceedings.

For further information and submission instructions see the conference's web page:

<http://www.iacr.org/workshops/pkc2015/>

## Deadlines:

Submission: Oct. 6, 2014 17:00 EST

Notification: Dec. 15, 2014

Camera-Ready: Jan. 11, 2015

An author of each accepted paper will be required to present the paper at the conference.

## Proceedings:

The PKC 2015 proceedings will be published in Springer's LNCS series.

## Conference Chairs:

Jonathan Katz (Program chair)

Rene Peralta (General chair)

## Program Committee:

Michel Abdalla	ENS & CNRS, France
Shweta Agrawal	I.I.T. Delhi, India
Melissa Chase	Microsoft Research, USA
Sherman S.M. Chow	Chinese Univ. of Hong Kong
Jean-Sébastien Coron	Univ. of Luxembourg
Jean-Charles Faugère	INRIA, France
Sebastian Faust	EPFL, Switzerland
Dario Fiore	IMDEA Software, Spain
Georg Fuchsbauer	IST Austria
Steven Galbraith	Univ. of Auckland, NZ
Pierrick Gaudry	LORIA, France
Matt Green	Johns Hopkins Univ., USA
Goichiro Hanaoka	AIST, Japan
Carmit Hazay	Bar-Ilan Univ., Israel
Jonathan Katz	Univ. of Maryland, USA
Eike Kiltz	Univ. Bochum, Germany
Benoit Libert	ENS Lyon, France
Shengli Liu	Shanghai Jiao Tong Univ.
Anna Lysyanskaya	Brown University, USA
Mark Manulis	University of Surrey, UK
Sarah Meiklejohn	Univ. College London, UK
Dustin Moody	NIST, USA
Michael Naehrig	Microsoft Research, USA
Adam O'Neill	Georgetown Univ., USA
Chris Peikert	Georgia Tech, USA
Dominique Schröder	Saarland Univ., Germany
Peter Schwabe	Radboud Univ., Netherlands
Jae Hong Seo	Myongji Univ., Korea
Damien Stehlé	ENS Lyon, France
Rainer Steinwandt	Florida Atlantic Univ., USA

Generously sponsored by: