

**Program Chair**

Marc Fischlin

**General Chair**

Johannes Buchmann

**General Co-Chair**

Mark Manulis

**Program Committee**

Michel Abdalla  
 Alexandra Boldyreva  
 Colin Boyd  
 Dario Catalano  
 Jean-Sebastien Coron  
 Marc Fischlin  
 Georg Fuchsbauer  
 Rosario Gennaro  
 Dov Gordon  
 Matthew Green  
 Jens Groth  
 Kaoru Kurosawa  
 Mirosław Kutylowski  
 Vadim Lyubashevsky  
 Adam O'Neill  
 Christiane Peters  
 Krzysztof Pietrzak  
 Alon Rosen  
 Dominique Schröder  
 Gil Segev  
 Nicolas Sendrier  
 Igor Shparlinski  
 Nigel Smart  
 Ron Steinfeld  
 Rainer Steinwandt  
 Tomas Toft  
 Wen-Guey Tzeng  
 Ivan Visconti  
 Scott Yilek  
 Yuliang Zheng

**Local Support**

Stanislav Bulygin

## PKC 2012 | Call for Papers

15th IACR International Conference on  
 Practice and Theory in Public-Key Cryptography

May 21-23, 2012, Darmstadt (Germany)  
[pkc2012.cased.de](http://pkc2012.cased.de)

The International Conference on Practice and Theory in Public-Key Cryptography (PKC) has been the main annual conference focusing on all aspects of public-key cryptography, attracting cutting-edge results from world-renowned scientists in the area. It is organized annually by the International Association for Cryptologic Research (IACR). The 15th edition of the conference will be held for the first time in Germany, organized by Center for Advanced Security Research Darmstadt (CASED). The conference will be held at the modern congress center Darmstadtium.



### Submissions

Original research papers on all technical aspects of public-key cryptography are solicited for submission to PKC 2012. Papers suggesting novel paradigms, original directions, or non-traditional perspectives are especially welcome.

Submission      **December 15, 2011, 11:00 UTC**  
 Notification     **February 27, 2012**  
 Camera-ready    **March 12, 2012**

Accepted papers will be published as a volume in Springer-Verlag's Lecture Notes in Computer Science (LNCS) series and will be available at the conference.

