

# The 14<sup>th</sup> IACR International Conference on Practice and Theory in Public Key Cryptography (PKC 2011)



**March 6-9, 2011**

**Taormina, Italy**

<http://www.iacr.org/workshops/pkc2011/>

## IMPORTANT DATES

**Submission deadline: October 1, 2010 17:00 EDT**

**Author notification:** November 24, 2010

**Camera-ready copy:** December 23, 2010

## GENERAL INFORMATION

Original research papers on all technical aspects of public-key cryptography are solicited for submission to PKC 2011, the 14th International Conference on Practice and Theory in Public Key Cryptography. Papers suggesting novel paradigms, original directions, or non-traditional perspectives are especially welcome.

## INSTRUCTIONS FOR AUTHORS

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or any work which has been submitted to another conference with proceedings and which is still under consideration for publication at that conference at any point in time before the author notification deadline (November 24, 2010). Parallel submissions will be rejected from all venues to which they have been submitted, and further actions may be taken!

A sharp limit of **12 pages**, not including, title page, references and appendices, in 11pt fonts, single column, with reasonable margins, is placed on all submissions. Note that the final version will be limited to 18 pages in the LNCS class format. The paper should be intelligible and self-contained without appendices, as committee members are not required to read them.

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. If accepted, one of the authors is expected to present the paper at the conference.

## PROCEEDINGS

Proceedings will be published in Springer-Verlag's LNCS series.



## CONFERENCE CHAIRS

**Program Chair:** Rosario Gennaro, IBM Research, USA

**General Chairs:** Nelly Fazio, City University of New York, USA

Antonio Nicolosi, Stevens Institute of Tech., USA

**Local Arrangements Chair:** Dario Catalano, U. di Catania, Italy

## PROGRAM COMMITTEE

Masayuki Abe, NTT Labs, Japan

John Black, University of Colorado, USA

Alexandra Boldyreva, Georgia Institute of Technology, USA

Colin Boyd, Queensland University of Technology, Australia

Emmanuel Bresson, EADS, France

Melissa Chase, Microsoft Research, USA

Paolo D'Arco, Università di Salerno, Italy

Alexander W Dent, Royal Holloway, University of London, UK

Mario Di Raimondo, Università di Catania, Italy

Stefan Dziembowski, Università di Roma "La Sapienza", Italy

Dario Fiore, École Normale Supérieure, France

Marc Fischlin, Technische Universität Darmstadt, Germany

Rosario Gennaro (**chair**), IBM Research, USA

Carmit Hazay, Aarhus Universitet, Denmark

Martin Hirt, ETH Zurich, Switzerland

Stanislaw Jarecki, University of California at Irvine, USA

Eike Kiltz, Ruhr-Universität Bochum, Germany

Kaoru Kurosawa, Ibaraki University, Japan

Yehuda Lindell, Bar-Ilan University, Israel

Sebastià Martin, Universitat Politècnica de Catalunya, Spain

Alexander May, Ruhr-Universität Bochum, Germany

Jesper Buus Nielsen, Aarhus Universitet, Denmark

Bryan Parno, Microsoft Research, USA

Mike Rosulek, University of Montana, USA

Guy Rothblum, IAS Princeton, USA

Kazue Sako, NEC, Japan

Berry Schoenmakers, Technische U. Eindhoven, The Netherlands

Thomas Shrimpton, Portland State University, USA

Nigel Smart, Bristol University, UK

Edlyn Teske, University of Waterloo, Canada

Muthu Venkatasubramanian, New York University, USA

## PKC STEERING COMMITTEE

Ronald Cramer, CWI & Universiteit Leiden, The Netherlands

Yvo Desmedt, University College London, UK

Hideki Imai, Chuo University & AIST, Japan

David Naccache, École Normale Supérieure, France

Tatsuaki Okamoto, NTT Labs, Japan

David Pointcheval, École Normale Supérieure, France

Moti Yung (Secretary), Google Inc. & Columbia University, USA

Yuliang Zheng (Chair), Univ. of North Carolina at Charlotte, USA

