12th IACR International Workshop on Practice and Theory in Public Key Cryptography (PKC) 2009

March 18-20, 2009, Irvine, CA, USA

DEADLINES:

- **Submission:** **Sept. 24, 11:59pm PST, 2008**
- **Notification:** Nov. 25, 2008
- **Camera-Ready:** Dec. 20, 2008

GENERAL INFORMATION:

Original research papers on all technical aspects of public key cryptography are solicited for submission to PKC 2009, the 12-th International Workshop on Practice and Theory in Public Key Cryptography.

SUBMISSION INSTRUCTIONS:

Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted/ is planning to submit before the author notification deadline to other conferences/workshops that have proceedings. Parallel submissions will be immediately rejected and the names of the authors involved will be shared with other conference in the field.

Each submission must be:

- At most **14 pages**, not including references and appendices, in 11pt font and with **reasonable margins**.
- Intelligible and self-contained without appendices (reviewers are not required to read them).
- Anonymous: no author names, affiliations, acknowledgments, or obvious references.

Submissions not meeting these criteria will be rejected.

If a submission is accepted, one of the authors is expected to present the paper at the workshop. Further submission instructions and an electronic submission portal are on the PKC'09 web page: http://www.ics.uci.edu/~pkc09/
The direct link to the submission server is:
https://secure.iacr.org/websubrev/pkc2009/submit/.

PROCEEDINGS:

PKC'09 proceedings be published in Sprinter-Verlag LNCS Series and will be available at the conference.

Conference Chairs: **Stanislaw Jarecki and Gene Tsudik,**
University of California at Irvine
Contact email: **pkc09 [AT] ics.uci.edu**

PROGRAM COMMITTEE:

Xavier Boyen	Voltage Security, USA
Christian Cachin	IBM Zurich, Switzerland
Jan Camenisch	IBM Zurich, Switzerland
Jung Hee Cheon	Seoul National U., South Korea
Jean-Sebastien Coron	U. of Luxembourg, Luxembourg
Nelly Fazio	CUNY, USA
Bao Feng	i2R, Singapore
Pierre-Alain Fouque	ENS, France
Juan Garay	AT&T Labs - Research, USA
Rosario Gennaro	IBM TJ Watson, USA
Amir Herzberg	Bar Ilan University, Israel
Marc Joye	Thomson R&D, France
Seny Kamara	Microsoft Research, USA
Aggelos Kiayias	University of Connecticut
Eike Kiltz	CWI, The Netherlands
Javier Lopez	University of Malaga, Spain
Breno de Medeiros	Google, USA
David Naccache	ENS, France
Jesper Buus Nielsen	Aarhus University, Denmark
Kenny Paterson	Royal Holloway, UK
Benny Pinkas	University of Haifa, Israel
David Pointcheval	ENS-CNRS-INRIA, France
Ahmed Reza-Sadeghi	Bochum University, Germany
Rei Safavi-Naini	University of Calgary, Canada
Nitesh Saxena	NYU Polytechnic Institute, USA
Berry Schoenmakers	TU Eindhoven, The Netherlands
Hovav Shacham	UCSD, USA
Vitaly Shmatikov	UT Austin, USA
Igor Shparlinski	Macquarie University, Australia
Michael Steiner	IBM TJ Watson, USA
Serge Vaudenay	EPFL, Switzerland
Ivan Visconti	University of Salerno, Italy
Suzanne Wetzel	Stevens Inst. of Technology, USA

PKC STEERING COMMITTEE:

Ronald Cramer	CWI, The Netherlands
Yvo Desmedt	University College London, UK
Hideki Imai	AIST, Japan
David Naccache	ENS, France
Tatsuyaki Okamoto	NTT, Japan
Jacques Stern	ENS, France