

WEWoRC 2009



July 7-9, Graz, Austria

Call for Papers

<http://www.weworc.org/>

WEWoRC 2009 is a research meeting in the field of cryptology. Topics of interest include, but are not limited to, the following:

- Foundations of cryptology (e.g., from computational number theory, complexity theory, combinatorics)
- Secret-key cryptosystems, hash functions
- Public-key cryptosystems
- Cryptanalysis
- Modes of operation (e.g., authenticated encryption and signcryption)
- Cryptographic protocols (e.g., privacy, mobile security, distributed cryptography)
- Hardware and software implementation of cryptosystems and their integration into secure systems
- Secure operating systems and trusted computing
- Electronic voting and elections systems
- Applications such as watermarking and code obfuscation

The workshop will be held in Graz, Austria. The workshop is organised by the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz). The chairs are Mario Lambergner and Christian Rechberger.

Those who wish to give a talk are invited to submit an extended abstract of 1-2 pages (short talk) or 3-5 pages (long talk). The workshop language is English, instructions for authors can be found on the workshop website.

Important dates for workshop:

Submission Deadline: Fr, June 5, 2009
Notification of Acceptance: Fr, June 12, 2009
Registration Deadline: Fr, June 19, 2009
Workshop: Tue-Thu, July 7-9, 2009

Important dates for post-conference proceedings:

Submission Deadline: Fr, September 25, 2009
Notification of Acceptance: Fr, November 20, 2009

Conference records will contain all abstracts submitted before the deadline and will be distributed during the workshop. In addition, they will be made available online through the workshop homepage. A number of selected articles will be published in post-proceedings. Here, emphasis is given to young researchers. The post-conference proceedings are planned to appear in the "Lecture Notes in Computer Science" (LNCS) series of Springer.

Program Committee:

Frederik Armknecht, Ruhr-University Bochum, DE
Olivier Billet, Orange Labs, FR
Carlos Cid, Royal Holloway, University of London, UK
Orr Dunkelman, ENS, FR
Jürgen Fuß, FH Hagenberg, AT
Stefan Katzenbeisser, TU Darmstadt, DE
Aggelos Kiayias, UConn, US
Mirosław Kutyłowski, Wrocław UT, PL
Eike Kiltz, CWI, NL
Gregor Leander, DTU, DK
Stefan Lucks, Bauhaus-Universität Weimar, DE
David Naccache, ENS, FR
Chris Mitchell, Royal Holloway, University of London, UK
Raphael Phan, Loughborough Uni, UK
Bart Preneel, KU Leuven, BE
Christian Rechberger, TU Graz, AT (chair)
Vincent Rijmen, TU Graz, AT, and KU Leuven, BE
Nicolas Sendrier, INRIA, FR
Martijn Stam, EPFL, CH
François-Xavier Standaert, UCL, BE
Michael Tunstall, University of Bristol, UK
Huaxiong Wang, NTU, SG
Christopher Wolf, HGI, Ruhr-University Bochum, DE