

WEWoRC 2011

4th Western European Workshop on Research in Cryptology

July 20—22, 2011
Weimar, Germany



A number of selected articles will be published in the post-proceedings. Here, the emphasis is given to junior researchers and their results. The post-proceedings are planned to appear in the Springer Lecture Notes (LNCS) series of Springer Verlag, like the post-proceedings of previous WEWoRC 2007 and 2009.

Dates:

Submission deadline: **Fr. June 12, 2011**
Notification of acceptance: **Fr. June 25, 2011**
Registration deadline: **Fr. July 01, 2011**
Workshop: **We—Fr July 20—22, 2011**
Submission deadline for post-conference proceedings: **Fr. September 30, 2011**

Invited Speakers:

Marc Fischlin (Technical University Darmstadt, Germany)
Heike Neumann (NXP Semiconductors)

WEWoRC is a research meeting in the field of cryptology with a specific focus on young researchers. Topics of interest include, but are not limited to

- Foundations of cryptology (e.g., from computational number theory, complexity theory, combinatorics)
- Secret-key cryptosystems and hash functions
- Public-key cryptosystems
- Modes of operation
- Cryptographic protocols
- Hardware and software implementation of cryptosystems and their integration into secure systems
- Applications such as watermarking and code obfuscation

The workshop will be held at Bauhaus-Universität Weimar in Weimar, Germany. The chairs are Frederik Armknecht and Stefan Lucks.

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. Observe that presenting does not prevent future or concurrent submission to any journal or conference with proceedings.

In addition to the call for presentation, this workshop will have invited speakers from industry and academia to share their experiences.

Program committee:

Frederik Armknecht (Universität Mannheim, Germany)
Jens-Matthias Bohli (NEC, Germany)
Carlos Cid (Royal Holloway, University of London, UK)
Orr Dunkelman (Weizmann Institute & University of Haifa, Israel)
Joachim von zur Gathen (b-it Bonn, Germany)
Willi Geiselmann (TU Karlsruhe, Germany)
Helena Handschuh (Intrinsic ID, Netherlands & KU Leuven, Belgium)
Florian Hess (Oldenburg, Germany)
Stefan Katzenbeisser (TU Darmstadt, Germany)
Gregor Leander, (DTU, Denmark)
Stefan Lucks, (Bauhaus-Universität Weimar, Germany)
Roel Maes (KU Leuven, Belgium)
Alexander May (RU Bochum, Germany)
Willi Meier (FHNW, Switzerland)
Heike Neumann, (NXP Semiconductors, Germany)
Thomas Peyrin (Nanyang Technological University, Singapore)
Bart Preneel (KU Leuven, Belgium)
Christian Rechberger (ENS, Paris, France)
Vincent Rijmen (TU Graz, Austria & KU Leuven, Belgium)
Ahmad-Reza Sadeghi (TU Darmstadt, Germany)
Rei Safavi-Naini (University of Wollongong, Australia)
Jean-Pierre Seifert (TU Berlin, Germany)
François-Xavier Standaert, (UCL, Belgium)
Christopher Wolf (HGI, RU Bochum, Germany)
Moti Yung (Columbia University & RSA Labs, USA)
Erik Zenner (DTU, Denmark)

<<http://2011.weworc.org>>