Call for Papers

WEWoRC 2015
6th Western European Workshop on Research in Cryptology

http://2015.weworc.org

October 1-2, 2015 in Cottbus, Germany

Co-located with the 45th Symposium of the German Computer Science Association GI (INFORMATIK 2015)

http://informatik2015.de/

General information

The Western European Workshop on Research in Cryptology (WEWoRC) is a bi-yearly international workshop with a specific focus on research performed by junior scientists in the area of cryptology. This focus is exhibited by the rule that at least one of the authors of a paper which is to be presented at WEWoRC must be a junior researcher.

Topics of interest include, but are not limited to:

- Foundations of cryptology (e.g., computational number theory, complexity theory, …)
- Secret-key cryptography (e.g., block ciphers, stream ciphers, hash functions, MACs, …)
- Public-key cryptography (e.g., identification protocols, digital signatures, encryption, …)
- Cryptanalysis
- Cryptographic protocols (e.g., privacy, mobile security, distributed cryptography, …)
- Design of cryptographic schemes
- Security proofs
- Anonymity (e.g., in e-commerce, e-voting, …)
- Implementation of cryptosystems and their integration into secure systems
- Secure operating systems and trusted computing
- Applications like watermarking or code obfuscation

The workshop is co-located with the 45th Symposium of the German Computer Science Association GI (INFORMATIK 2015). This year's chair is Andreas Peter. 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 can be found on the workshop web site. Conference records will contain all abstracts accepted for presentation at the workshop and will be made available at the workshop.

Submissions of abstracts must not be anonymized!

Important dates

Submission deadline:	~~**Wed, May 13, 2015**~~
(extended)	**Wed, Jun 3, 2015**
Notification of acceptance:	**Wed, Jun 17, 2015**
Workshop:	**Thu-Fri, Oct 1-2, 2015**

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 will appear in the Lecture Notes in Informatics (LNI) series of the GI.

Submission deadline for the post-proceedings: **Fri, Dec 4, 2015**

Program committee

- Frederik Armknecht (University of Mannheim, DE)
- Jens-Matthias Bohli (NEC, DE)
- Colin Boyd (NTNU, NO)
- Carlos Cid (RHUL, UK)
- Maarten Everts (TNO, NL)
- Willi Geiselmann (KIT Karlsruhe, DE)
- Gottfried Herold (RU Bochum, DE)
- Stefan Katzenbeisser (TU Darmstadt, DE)
- Aggelos Kiayias (University of Athens, GR)
- Stefan Lucks (Bauhaus-University Weimar, DE)
- Mark Manulis (University of Surrey, UK)
- David Naccache (ENS, FR)
- Kenny Paterson (RHUL, UK)
- Andreas Peter (University of Twente, NL) **(chair)**
- Christiane Peters (ENCS, NL)
- Thomas Peyrin (NTU, SG)
- Bart Preneel (KU Leuven, BE)
- Vincent Rijmen (KU Leuven, BE)
- Francois-Xavier Standaert (UCL, BE)
- Susan Thomson (University of Bristol, UK)
- Erik Zenner (Uni of Applied Sc. Offenburg, DE)