The Second International Workshop on Modern Cryptography and Security Engineering

MoCrySEn 2013 - Preliminary Call For Papers

Aims and Objective

The Second International Workshop on Modern Cryptography and Security Engineering (co-located with the International Conference on Availability, Reliability and Security) aims to bring together researchers working in theoretical aspects of modern cryptography (including but not restricted to design and analysis of symmetric-key primitives and cryptosystems, block and stream ciphers, hash functions and MAC algorithms, efficient implementations and analysis of public-key cryptosystems, public-key signatures, threshold schemes) with professionals working on applied aspects of security engineering, particularly people involved in standardization and in industrial deployment of cryptography (encryption schemes for databases and related security, cryptography in wireless applications, hardware for cryptanalysis, digital signatures, FPGA and smart cards security). The main goal of the workshop is to strengthen the dialogue between these two groups, which is currently perceived to be weak. Ultimately, we aim to continue bridging the gap between what academic cryptographers believe should be the goals of cryptographic design and what is actually implemented in the real world. MoCrySEn intends to provide a better understanding of real-world cryptographic issues to the theoretical community, helping to inform their research and set new research challenges for the theoretical community and enable practitioners to develop a clearer view of the current state-of-the-art in cryptographic research and what it offers to practitioners.

Topics of Interest

include, but are not limited to:

- Symmetric cryptography
- Public-key cryptography
- Secret-sharing cryptography
- Algorithmic cryptanalysis
- Database encryption
- Public-key signatures
- Software and hardware implementation of cryptographic algorithms
- Hardware security
- Cryptographic schemes for mobile devices
- Interactions between cryptographic theory and implementation issues

Important Dates

- **Submission Deadline**: April 30th, 2013
- Author Notification: May 31st, 2013
- Proceedings Version: June 11st, 2013
- Conference: September 2th - 6th, 2013

Workshop Chairs

- Dimitris E. Simos, INRIA, France (Chair)
  Contact: dimitrios.simos@inria.fr
- Nicolas Sendrier, INRIA, France (Co-Chair)
  Contact: nicolas.sendrier@inria.fr
- Edgar Weippl, SBA Research, Austria (Co-Chair)
  Contact: eweippl@sba-research.org

Program Committee

- Athanasios Angelakis, Leiden University, Netherlands, Universite Bordeaux 1, France
- Paulo Barreto, Universidade de Sao Paulo, Brazil
- Christina Boura, Technical University of Denmark, Denmark
- Pierre-Louis Cayrel, Universite Jean Monnet, France
- Matthieu Finiasz, CryptoExperts, France
- Stefan Heyse, Ruhr-Universitat Bochum, Germany
- Aleksandar Hudic, SBA Research, Austria
- Peter Kieseberg, SBA Research, Austria
- Christos Koukouvinos, National Technical University of Athens, Greece
- Spyros Magliveras, Florida Atlantic University, USA
- Ayoub Otmani, University of Rouen, France
- Christiane Peters, Technical University of Denmark, Denmark
- Ludovic Perret, Universite Pierre et Marie Curie 06 / INRIA, France
- Maria Naya-Plasencia, INRIA, France
- Jean-Pierre Tillich, INRIA, France
- Zlatko Varbanov, Veliko Tarnovo University, Bulgaria
- Amr Youssef, Concordia Institute for Information System Engineering, Canada

Submission Guidelines

As MoCrySEn is co-located with the ARES conference http://www.ares-conference.eu, anonymized submissions are required, in order to ensure a double blind review. In addition, submitted papers must conform to the "Springer LNCS Series" format http://www.springer.de/comp/lncs/authors.html and they must not exceed more than **12** pages, excluding well-marked appendices and bibliography. For more details, regarding the submission procedure please consult the workshop's webpage at http://mocrysen2013.inria.fr or contact the workshop chairs.

Proceedings

All accepted papers of the workshop will be published by **Springer Lecture Notes in Computer Science (LNCS)** with IFIP logo (indexed by EI) joint with the proceedings of the CD-ARES conference. The proceedings will be available at the workshop. At least one author of an accepted paper must register at the ARES 2013 site and present the paper at the workshop.

To be held at September 2th-6th, 2013 in University of Regensburg, Germany