

SKEW 2011

Symmetric Key Encryption Workshop

Collocated with FSE 2011

February 16–17, 2011

Lyngby, Denmark

Call for Papers

After an interruption of three years, SKEW 2011 will become the sixth in a series of ECRYPT workshops dedicated to symmetric-key encryption techniques. Continuing in the tradition of the previous SASC/SKEW workshops, SKEW 2011 will provide a forum for discussing the most recent developments in the field of stream ciphers. However, as opposed to earlier editions, this year's workshop intends to cover other aspects of symmetric-key encryption as well, ranging from new theoretical insights in block cipher cryptanalysis, to the design, implementation and deployment of encryption algorithms for/in severely constrained environments.

SKEW 2011 encourages submissions on any topic related to symmetric-key encryption.¹ This includes, but is not limited to:

- design or analysis of stream ciphers and block ciphers,
- implementations of symmetric-key encryption algorithms,
- reports on the deployment of symmetric-key encryption techniques in real-world applications,
- updates on industry requirements with respect to symmetric-key encryption.

In order to prevent submissions to SKEW 2011 from conflicting with submissions to forthcoming conferences with proceedings, SKEW 2011 will have no formal proceedings, but a conference record will be available.

Important Dates

Submission deadline:	January 10, 2011
Notification:	January 24, 2011
Workshop:	February 16–17, 2011

General co-Chairs

Gregor Leander, Technical University of Denmark
Søren S. Thomsen, Technical University of Denmark

Program co-Chairs

Gregor Leander, Technical University of Denmark
Søren S. Thomsen, Technical University of Denmark

¹Note that hash functions are *not* considered to be encryption algorithms.

Program Committee

Steve Babbage, Vodafone, UK
Alex Biryukov, University of Luxembourg
Andrey Bogdanov, K.U.Leuven, Belgium
Julia Borghoff, DTU, Denmark
Anne Canteaut, INRIA, France
Carlos Cid, Royal Holloway, UoL, UK
Joan Daemen, STMicroelectronics, Belgium
Christophe De Cannière, K.U.Leuven, Belgium
Henri Gilbert, ANSSI, France
Christoph Herbst, NXP Semiconductors Austria
Sebastiaan Indestege, K.U.Leuven, Belgium
Thomas Johansson, Lund University, Sweden
Emilia Käsper, K.U.Leuven, Belgium
Dmitry Khovratovich, Microsoft Research, USA
Andreas Klein, UGent, Belgium
Mario Lamberger, TU Graz, Austria
Stefan Mangard, Infineon Technologies, Germany
Willi Meier, FHNW, Switzerland
Maria Naya-Plasencia, FHNW, Switzerland
Mastooreh Negin Salajegheh, UMass Amherst, USA
Matthew Parker, University of Bergen, Norway
Christian Rechberger, K.U.Leuven, Belgium
Matt Robshaw, Orange Labs, France
Patrick Schaumont, Virginia Tech, USA
Martin Schläffer, TU Graz, Austria
François-Xavier Standaert, UC Louvain, Belgium
Dai Watanabe, Hitachi, Japan
Hongjun Wu, NTU, Singapore

For contact information, details of the submission procedures, or other practical information, please visit the SKEW 2011 website:

<http://skew2011.mat.dtu.dk>.