

SPECIAL WORKSHOP TO BE HOSTED BY THE ECRYPT NETWORK OF EXCELLENCE

SASC 2008

State of the Art of Stream Ciphers

February 13–14, 2008
Lausanne, Switzerland

Call for Participation

SASC 2008 is the fourth ECRYPT workshop dedicated to the state of the art of stream ciphers. The first workshop, organized in October 2004, discussed general security aspects of stream ciphers, the second and third workshops were mostly concerned with eSTREAM candidates.

SASC 2008 will provide a forum for the exchange of ideas about all aspects of stream ciphers. Particular attention will be focused on submissions to eSTREAM and we expect papers and discussions at SASC 2008 to be helpful in identifying the most promising stream ciphers in the final phase.

Submissions to SASC 2008 are encouraged on any topic related to stream ciphers. These might include, but are not limited to:

- stream cipher analysis, particularly for candidates to eSTREAM,
- stream cipher implementation, particularly for candidates to eSTREAM,
- stream cipher deployment, and
- stream cipher building blocks.

We also encourage submissions that question or comment upon:

- the need for, and desirability of, trusted stream ciphers, and
- the requirements of industry.

To avoid submissions to SASC 2008 from conflicting with submissions to forthcoming conferences with proceedings, SASC 2008 will have no formal proceedings though there will be a research record.

Important Dates

Submission deadline:	January 11, 2008
Notification:	January 25, 2008
Workshop:	February 13–14, 2008

Details of the program committee, submission procedures and workshop logistics will become available via

<http://www.ecrypt.eu.org/stvl/sasc2008>.