

SPECIAL WORKSHOP TO BE HOSTED BY THE ECRYPT NETWORK OF EXCELLENCE

# SASC 2006

## *Stream Ciphers Revisited*

February 2-3, 2006

Leuven, Belgium

### *Call for Participation*

In October of 2004, the *ECRYPT Network of Excellence* (<http://www.ecrypt.eu.org>) sponsored the SASC workshop to highlight the state of stream cipher design and analysis. In SASC 2006 we will meet again to consider how the state of stream ciphers might be changing, particularly now that more than thirty stream ciphers have been proposed within *eSTREAM* (<http://www.ecrypt.eu.org/stream/>).

SASC 2006 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 2006 to be helpful in identifying the most promising stream ciphers for Phase II of *eSTREAM*.

Submissions to SASC 2006 are encouraged on any topic of relevance 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,
- stream cipher building blocks, and
- stream cipher proposals and tweaks to *eSTREAM* candidates (accompanied by appropriate security claims and analysis).

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 2006 from conflicting with submissions to forthcoming conferences with proceedings, SASC 2006 will have no formal proceedings though there will be a workshop record. Depending on the number of submissions, papers directly related to *eSTREAM* may take precedence.

|                          |               |            |
|--------------------------|---------------|------------|
| <b>Program Chair:</b>    | Anne Canteaut | INRIA      |
| <b>Organising Chair:</b> | Joseph Lano   | K.U.Leuven |

Details on submission and workshop logistics will be available at <http://www.ecrypt.eu.org/stvl/sasc2006>.

### Important Dates

|                                 |                    |
|---------------------------------|--------------------|
| <b>Submission Deadline:</b>     | January 2, 2006    |
| <b>Submission Notification:</b> | January 12, 2006   |
| <b>Workshop:</b>                | February 2-3, 2006 |