SPECIAL WORKSHOP TO BE HOSTED BY THE ECRYPT NETWORK OF EXCELLENCE IN CRYPTOLOGY

SASC 2007

THE STATE OF THE ART OF STREAM CIPHERS

January 31-February 1, 2007

Bochum, Germany

Call for Papers

In October of 2004, the ECRYPT Network of Excellence in Cryptology initiated the SASC workshop to highlight the state of stream cipher design and analysis. In SASC 2007, the third in the series of SASC workshops, we will meet again to consider how the state of stream ciphers might be changing, with special focus on stream ciphers that have been proposed within eSTREAM.

SASC 2007 will provide a forum for the exchange of ideas about all aspects of stream ciphers. Particular attention will be focused on submissions present in the second phase of eSTREAM and we expect papers and discussions at SASC 2007 to be helpful in identifying the most promising stream ciphers for further evaluation.

Submissions to SASC 2007 are encouraged on any topic of relevance to stream ciphers. These might include, but are not limited to:

- stream cipher analysis, particularly for candidates in the second phase of eSTREAM,
- stream cipher implementation, particularly for candidates in the second phase of eSTREAM,
- any issues in connection with the evaluation of candidates in the second phase of eSTREAM,
- stream cipher design and deployment.

We also encourage submissions that question or comment upon

- the need for, and desirability of, trusted stream ciphers, and,
- the (functional and security) requirements of applications.

Workshop Record

To avoid submissions to SASC 2007 from conflicting with submissions to forthcoming conferences with proceedings, SASC 2007 will have no formal proceedings though there will be a workshop record.

Program Chair

Thomas Johansson	Lund University, Sweden

Program Committee

Steve Babbage	Vodafone, UK
Christophe De Canniere	Katholieke Universiteit Leuven, Belgium
Anne Canteaut	INRIA, France

Carlos Cid	Royal Holloway, University of London, UK
Henri Gilbert	France Telecom R&D, France
Thomas Johansson	Lund University, Sweden
Christof Paar	Ruhr-University of Bochum, Germany
Matthew Parker	University of Bergen, Norway
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Matt Robshaw	France Telecom R&D, France
Hongjun Wu	Katholieke Universiteit Leuven, Belgium

Local Organization

Kerstin Lemke-Rust	Ruhr University Bochum, Bochum, Germany
Christof Paar	Ruhr University Bochum, Bochum, Germany

E-mail: SASC2007@crypto.rub.de
Web: http://sasc.crypto.rub.de/

Submission: Submission details are available on http://www.ecrypt.eu.org/stvl/sasc2007/submission.html.

Important Dates: **Submission Deadline:** January 2, 2007,
Notification: January 12, 2007,
Final Version: January 19, 2007