

Update on eSTREAM and SASC 2007

ECRYPT Network of Excellence

November 24, 2006

`estream@ecrypt.eu.org`

Thank you to everyone that has contributed to the eSTREAM project so far. The aim of eSTREAM is to identify a small portfolio of stream ciphers that will be of interest to the cryptographic community and potentially to standards bodies. While such ciphers won't be formally approved by ECRYPT¹, they are likely to mark a significant advance in the development of stream ciphers and to represent some of the most promising contemporary proposals. The next steps in eSTREAM are outlined below.

SASC 2007

Preparations for SASC 2007 are well underway. It will be held in Bochum, Germany on January 31 and February 1 2007. Workshop and submission details are available via www.ecrypt.eu.org/stream.

There will be ample time at the workshop for open discussions on a variety of topics. A number of issues have already been identified, including IP, but if there are any particular issues of general interest to eSTREAM that you feel might be discussed please send an email to `estream@ecrypt.eu.org`.

Assessment of eSTREAM Candidates

When moving from Phase I to Phase II we stressed the need for a periodic reassessment of the candidates. We will use SASC 2007 as the starting point for the next reassessment and hope to announce a new classification of candidates by the end of March. During this reassessment we will be as fair and as objective as we can, but our decision is likely to depend on issues such as:

- 1. Security**
- 2. Performance when compared to the AES and other submissions**
- 3. Justification and supporting analysis**
- 4. Simplicity and flexibility**
- 5. Completeness and clarity of submission**

Submissions with identified security issues cannot be expected to advance. We may also take into account certification attacks that demonstrate deviation from the ideal cipher model, even if the practical impact is currently limited.

¹ ECRYPT is a Network of Excellence within the Information Societies Technology (IST) Programme of the European Commission. The information in this note is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at his or her sole risk and liability.

Intellectual Property Statements

If you have made changes to any IP statements, please be sure that the details are known to the project administrators at estream@ecrypt.eu.org.

Software Performance Testing

We will conduct another round of software performance evaluation. An email will shortly be sent to submitters with more details.

1. Since the results are likely to be academically interesting, we will measure the software performance of all Phase II ciphers. However, the results will only be applied to those that are claimed to be suitable for Profile I.
2. The submitters of tweaked candidates may have sent reference (i.e. unoptimised) code at the start of Phase II. For this reason any submitters can submit additional optimised code by January 15, 2007.
3. We will test the most recent, single version of the code that is available to us on January 15, 2007. We will therefore use the code that accompanied the submission and/or tweak as a default.
4. Tweaked submissions that are not accompanied by functioning reference code at a minimum, run the risk of rejection from eSTREAM.

Hardware Performance Testing

It is anticipated that submissions to SASC 2007 will help to provide additional new information on this issue. Thus third party analysis and contributions on hardware performance are particularly welcome.

Feedback and Comments

Please send any feedback or comments to estream@ecrypt.eu.org.