IST-2002-507932

ECRYPT

European Network of Excellence in Cryptology

Network of Excellence
Information Society Technologies

D.STVL.1

eSTREAM -
Stream Cipher Proposals for Ongoing Analysis

Due date of deliverable: 31. January 2006
Actual submission date: 16. February 2006

Start date of project: 1. February 2004
Duration: 4 years

Lead contractor: Katholieke Universiteit Leuven (KUL)

Revision 1.0

<table>
<thead>
<tr>
<th>Dissemination Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
</tr>
<tr>
<td>PP</td>
</tr>
<tr>
<td>RE</td>
</tr>
<tr>
<td>CO</td>
</tr>
</tbody>
</table>

Project co-funded by the European Commission within the 6th Framework Programme
eSTREAM -
Stream Cipher Proposals for Ongoing Analysis

Editor
Thomas Johansson (LUND)

Contributors
Joseph Lano (KUL), Matt Robshaw (FTRD)

16. February 2006
Revision 1.0

The work described in this report has in part been supported by the Commission of the European Communities through the IST program under contract IST-2002-507932. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.
Contents

1 Introduction 1

2 Technical Background 3
   2.1 The Original Call for Primitives 4
   2.2 Formal Submission Requirements 6

3 Result of the Call 9

4 First Phase Analysis 11
   4.1 Cryptanalysis of Submitted Stream Ciphers 11
   4.2 Software Performance Evaluation for Stream Ciphers in Profile I (SW) 12
   4.3 Hardware Performance Evaluation for Stream Ciphers in Profile II (HW) 13

5 The Next Steps 15
Chapter 1

Introduction

The ECRYPT Stream Cipher Project, abbreviated eSTREAM, is a multi-year effort to identify new stream ciphers potentially suitable for widespread adoption.

All information on this project can be found via the Web site http://www.ecrypt.eu.org/stream/. The project is ongoing and in this brief report we provide information on the opening stages. It is anticipated that eSTREAM will run until the end of ECRYPT and thus will take around two more years to complete.

The anticipated result is a small portfolio of stream ciphers that have been available to cryptanalysis for several years and yet remain secure and of interest for implementation. Of course ECRYPT NoE is not a standardisation body, though the work in eSTREAM is likely to be of considerable interest to standardisation bodies. The resources developed within eSTREAM will be available to developers, implementers, and researchers alike and consist of specifications, implementation information, and research results. Throughout the duration of the project, comments from industry and the results of work in the research community are actively sought. At notable points during the process ECRYPT prepares and publishes updates on the progress of the submitted algorithms.

At the ECRYPT workshop State of the Art of Stream Ciphers, SASC, eSTREAM initiated an analysis of the general requirement of future stream ciphers. Thus took input from many interested parties, especially industry. In late 2004 eSTREAM announced a call for new stream cipher proposals with a deadline for submissions of April 2005.

The call resulted in a huge interest in the project and no less than 34 different stream cipher proposals were submitted in two different performance profiles. In connection to the call for proposals, ECRYPT has hosted two workshops in addition to SASC, Symmetric Key Encryption Workshop (SKEW) and Stream Ciphers Revisited (SASC2006). At each event many aspects of eSTREAM and stream cipher design and analysis were intensively discussed.

As ECRYPT does not provide the resources to perform the actual scientific analysis and evaluation of the received proposals, ECRYPT partners within eSTREAM act as a central node maintaining all the information created by different researchers, including algorithm descriptions and implementation, papers describing cryptanalysis and performance evaluation in software and hardware as well as designers proposed modifications to proposals. The current eSTREAM database (http://www.ecrypt.eu.org/stream/) contains 112 papers directly related to the eSTREAM project as well as two workshop records (SASC 2004 and SASC 2006). The eSTREAM project has additionally developed a framework for the fair testing the software proposals, something that is already being used by researchers outside of eSTREAM.
and outside of ECRYPT. There is also a Web-based discussion forum, with several hundred postings related to eSTREAM. Thus it is the input of the cryptographic community at large that will point to the most suitable stream cipher within eSTREAM.

After less than a year of analysis, more than half of the proposals have demonstrated weaknesses of various kinds. Designers have been encouraged to propose tweaks to their proposals if this will improve their security properties and/or performance.

Even during the first stage of the project, a huge amount of attention is being generated worldwide. As an example, more than 20% of the forthcoming Fast Software Encryption Workshop (FSE) will consist of papers that are directly related to eSTREAM candidates.

At this moment, the project will move to a second phase, focusing the attention to a subset of the submitted proposals. The details around the second phase are based on general discussion on e.g. the SASC 2006 workshop and will be finalized by an internal committee. The decision will be announced in March 2006.
Chapter 2

Technical Background

After an initial inventory of the general requirement of future stream ciphers, including input from industry, eSTREAM finalized an interest in stream cipher proposals suited to at least one of the stream cipher PROFILES listed below:

- PROFILE 1. Stream ciphers for software applications with high throughput requirements.

- PROFILE 2. Stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption.

Some arguments emphasized the importance of including an authentication method and so two further profiles are also proposed:

- PROFILE 1A. Stream ciphers satisfying PROFILE 1 with an associated authentication method.

- PROFILE 2A. Stream ciphers satisfying PROFILE 2 with an associated authentication method.

To launch this initiative, algorithm designers were invited to submit new stream cipher proposals to eSTREAM in a call for primitives. The deadline for this was set to April 29, 2005.

Our aim in eSTREAM is to identify a small portfolio of stream ciphers of interest to the community, including standards bodies. While such ciphers will not be formally approved by ECRYPT, they are likely to mark a significant advance in the development of stream ciphers and to represent some of the most promising contemporary proposals.

A (provisional) timetable of events associated with eSTREAM has been established as follows. Obviously, events may be added or changed.

- October 14-15, 2004. A workshop is hosted by ECRYPT in Bruges, Belgium: SASC - The State of the Art of Stream Ciphers. Discussion at this workshop leads to the ECRYPT Call for Primitives.

- November 2004. ECRYPT launches its Call for Primitives.

- April 29, 2005. The deadline of submission to ECRYPT. 34 primitives have been submitted to ECRYPT.
• May 26-27, 2005. A workshop is hosted by ECRYPT in Aarhus, Denmark: SKEW - Symmetric Key Encryption Workshop. At this workshop, 25 papers are presented, including 21 stream ciphers submitted to ECRYPT.

• June 13th, 2005. The eSTREAM Web site is launched, to promote the public evaluation of the primitives.


• February 2006. The end of the first evaluation phase of eSTREAM. The selection of candidates for evaluation in Phase II to be announced in March 2006.

• July 2006. The beginning of the second evaluation phase of eSTREAM.

• September 2007. The end of the second evaluation phase of eSTREAM.

• January 2008. The final report of eSTREAM.

2.1 The Original Call for Primitives

The original call for primitives outlined the process in the following way.

There will be two phases to the ECRYPT Stream Cipher project. The first phase will concentrate on accumulating information related to the submitted stream ciphers. At the end of the first phase, it is likely that a subset of the first phase ciphers will be advanced to the second phase. This will provide further focus to ongoing analysis within the cryptographic community. Since the goal of the project is to derive good stream ciphers, it is likely that potentially significant “tweaks” will be permitted in moving to the second phase.

ECRYPT solicited stream cipher proposals suited to at least one of the stream cipher PROFILES listed below:

• PROFILE 1. Stream ciphers for software applications with high throughput requirements.

• PROFILE 2. Stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption.

Two further profiles were proposed:

• PROFILE 1A. Stream ciphers satisfying PROFILE 1 with an associated authentication method.

• PROFILE 2A. Stream ciphers satisfying PROFILE 2 with an associated authentication method.

The main evaluation criteria are likely to be long-term security, efficiency (performance), flexibility and market requirements. Security is the most important criterion since it is essential to achieve confidence and build consensus. The performance of the primitive in the specified environment is important. For software, the range of environments may include 8-bit processors (as found in inexpensive smart cards), 32-bit processors (e.g., the Pentium
family) to the modern 64-bit processors. For hardware, both FPGAs and ASICs may be considered. We anticipate that different ciphers will perform best against different profiles; however, within any one profile, some flexibility of implementation is likely to be important, so that the range of environments in which it can be used is not unnecessarily restricted. Market requirements are related to the need for a primitive, its usability, and the possibility for world-wide use.

- **Security Criteria:**
  Any key-recovery attack (including time-memory-data tradeoff attacks) should be at least as difficult as exhaustive search. Also, distinguishing attacks are likely to be of interest to the cryptographic community. However the relative importance of high complexity distinguishing attacks may become an issue for wider discussion. Clarity of design is likely to be an important consideration.

- **Implementation Criteria:**
  Software and hardware efficiency will be compared with similar submissions and existing primitives. Execution code and memory sizes will be assessed according to their relevance in different contexts. Submitted primitives will be assessed against claimed performance, though it is clearly preferable for primitives to offer wide flexibility of use.

- **Licensing Requirements:**
  The submitter should state the position concerning intellectual property. This statement should be updated when necessary.

- **Submission Requirements:**
  For the ECRYPT NoE a stream cipher takes as input a message stream (M), a key (K), an initial value (IV), optionally for profiles that provide authentication, some associated data (AD).

  For the ECRYPT NoE a stream cipher gives as output a ciphertext stream (C), For profiles providing authentication, an authentication tag (AU), optionally for profiles that provide authentication, authenticated but unencrypted associated data (AU-AD).

- For stream ciphers without an authentication mechanism, the required parameter values are given below.
  - **PROFILE 1:**
    A key length of 128 bits must be accommodated. An IV length of at least one of 64 or 128 bits must be accommodated.

  - **PROFILE 2:**
    A key length of 80 bits must be accommodated. An IV length of at least one of 32 or 64 bits must be accommodated.

- For stream ciphers with an authentication mechanism, the required parameter values are given below.
  - **PROFILE 1A:** A key length of 128 bits must be accommodated. An IV length of at least one of 64 or 128 bits must be accommodated. An authentication tag length of at least one of 32, 64, 96, or 128 bits must be accommodated.
– **PROFILE 2A.** A key length of 80 bits must be accommodated. An IV length of at least one of 32 or 64 bits must be accommodated. An authentication tag length of at least one of 32 or 64 bits must be accommodated.

The following additional information was also useful in setting the expectations for eSTREAM.

- A stream cipher can be either synchronous or self-synchronising. While some IV sizes are specified as must-satisfy values, the ability to handle smaller IV spaces without hindering performance would be welcome.

- For any PROFILE it is likely that the stream cipher must be demonstrably superior to the AES in at least one significant aspect. Here we assume that the AES is used in some appropriate mode (e.g. counter mode). Time-memory trade-offs mean that the size of the stream cipher state should be appropriate for the claimed security level. For instance, the state size should be at least twice the key size. While attacks such as related-key attacks might not be directly addressed, they would be of considerable relevance to the ongoing assessment of the cipher. Issues such as side-channel analysis and secure implementation are likely to be a relevant consideration. In addition to theoretic estimations of the security of a cipher, full cost estimates of attacks might also be considered.

### 2.2 Formal Submission Requirements

Submissions to eSTREAM were required to include a primitive specification and supporting documentation, including a complete and unambiguous description of the primitive in the most suitable forms, such as a mathematical description, a textual description with diagrams, or pseudo-code. The specification of a primitive using code was not permitted.

The specification should include:

- a statement that there are no hidden weaknesses inserted by the designers;
- a statement of the claimed security properties and expected security level together with an analysis of the primitive;
- a statement giving the strengths and advantages of the primitive;
- a design rationale explaining design choices;
- a statement of the estimated computational efficiency in software; optionally the designers may provide estimates for performance in hardware; and
- a description of the basic techniques for implementers to avoid implementation weaknesses.

Submitters were also required to include implementations and test values, including a reference implementation in portable C satisfying the ECRYPT NoE specified API, a sufficient number of test vectors, and optionally, an optimized implementation for some architectures, a JAVA implementation, and an assembly language implementation.
Finally, an intellectual property statement giving the position concerning the intellectual property position and the royalty policy for the primitive was required.

Submissions had to arrive at the ECRYPT coordinator on, or before, April 29, 2005.
Chapter 3

Result of the Call

The call for primitives resulted in 34 candidates to eSTREAM. These designs are all publicly available on the eSTREAM Web site. The names of the submissions in each profile can be found in Table 3.1.
<table>
<thead>
<tr>
<th>Profile I</th>
<th>Profile I and II</th>
<th>Profile II</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>F-FCSR</td>
<td>Achterbahn</td>
</tr>
<tr>
<td>CryptMT/Fubuki</td>
<td>Hermes8</td>
<td>DECIM</td>
</tr>
<tr>
<td>DICING</td>
<td>LEX</td>
<td>EDON-80</td>
</tr>
<tr>
<td>DRAGON</td>
<td>MAG</td>
<td>Grain</td>
</tr>
<tr>
<td>Frogbit</td>
<td>NLS</td>
<td>MICKEY</td>
</tr>
<tr>
<td>HC-256</td>
<td>Phelix</td>
<td>MICKEY-128</td>
</tr>
<tr>
<td>Mir-1</td>
<td>Polar Bear</td>
<td>MOSQUITO</td>
</tr>
<tr>
<td>Py</td>
<td>POMARANCH</td>
<td>SFINKS</td>
</tr>
<tr>
<td>SOSEMANUK</td>
<td>Rabbit</td>
<td>Trivium</td>
</tr>
<tr>
<td></td>
<td>SSS</td>
<td>TSC-3</td>
</tr>
<tr>
<td></td>
<td>TRBDK3 YAEA</td>
<td>VEST</td>
</tr>
<tr>
<td></td>
<td>Yamb</td>
<td>WG</td>
</tr>
<tr>
<td></td>
<td>Salsa20</td>
<td>ZK-Crypt</td>
</tr>
</tbody>
</table>

Table 3.1: The submissions to eSTREAM with optional authentication method labelled.
Chapter 4

First Phase Analysis

The main evaluation criteria are likely to be long-term security, efficiency (performance), flexibility, simplicity and market requirements. Security is the most important criterion since it is essential to achieve confidence and build consensus.

Yet, the performance of a primitive is in some ways easier to determine and, using the AES process as a guide, it is typically the focus of many researchers. For software, the range of environments may include 8-bit processors (as found in inexpensive smart cards), 32-bit processors (e.g., the Pentium family) to the modern 64-bit processors. For hardware, both FPGAs and ASICs may be considered.

We anticipate that different ciphers will perform best against different profiles; however, within any one profile, some flexibility of implementation is likely to be important, so that the range of environments in which it can be used is not unnecessarily restricted. Market requirements are related to the need for a primitive, its usability, and the possibility for world-wide use.

4.1 Cryptanalysis of Submitted Stream Ciphers

Security criteria include resistance against any key-recovery attack (should roughly be at least as difficult as exhaustive search). Also, distinguishing attacks are of interest to the cryptographic community. However the relative importance of high complexity distinguishing attacks is an issue for wider discussion. Clarity of design is also an important security consideration.

As previously stated, the eSTREAM database contains 112 papers (see the Web site, list of all papers). More than half of them are papers on cryptanalysis of some submitted proposal. After less than a year of analysis, more than half of the proposals have demonstrated weaknesses of various kinds. Designers have been encouraged to propose tweaks to their proposals if this will improve their security properties and/or performance. The cryptanalysis work performed on a specific proposal can be found on the eSTREAM Web site (under CANDIDATES). Here it is listed all papers related to each proposal.

In general, it is quite difficult to grade the security of each proposal and possible tweaked versions based on the collected cryptanalysis papers. The relevance of certain attacks is also a topic of discussion. In moving to the second phase, this evaluation is left to the internal committee and will be performed in a manner resembling the work of a program committee for a conference. Other criteria will also be considered in this process. We refer the reader to
4.2 Software Performance Evaluation for Stream Ciphers in Profile I (SW)

One of the requirements imposed on all eSTREAM stream cipher submissions was that they should demonstrate the potential to be superior to the AES in at least one significant aspect. An aspect which is particularly significant for Profile I candidates is software performance. Software performance can be measured in many different ways, and in order to make comparisons as fair as possible, eSTREAM decided to develop a testing framework. This testing framework and documentation is now available at the eSTREAM Web site.

The framework has two objectives, assuring that all stream cipher proposals are submitted to the same tests under the same circumstances; and automating the test procedure as much as possible such that new optimized implementations can be included and tested with as little effort as possible.

The testing framework consists of a collection of scripts and C-code which test three aspects of the submitted code: API compliance, correctness, and performance. Many of these tests have been borrowed from the NESSIE Test Suite.

The latest results for all submissions, measured by eSTREAM on various platforms, can be found on eSTREAM Web site (in eSTREAM Software Performance testing, Section 6). We refer the reader to the Web site for the actual performance result for the different proposals on various platforms. As an illustration, we list the encryption speed (in cycles/byte) for the 10 proposals which perform best on a Pentium 4 for stream encryption, and also give their figures for the encryption of 576-byte frames, in Table 4.1. These figures are just given as an illustration, it does not reflect any preference of ECRYPT for this processor as a benchmark, for these stream ciphers or for these encryption benchmarks.
4.3 Hardware Performance Evaluation for Stream Ciphers in Profile II (HW)

Hardware evaluation is a much more difficult subject than evaluating software performance.

At SASC 2006 three papers on hardware implementation of the eSTREAM candidates were presented. This workshop provided interesting and lively discussions where hardware designers were confronted by the developers of the algorithms.

Some indications of the hardware performance for certain proposals could be established, but still many of them were not considered in enough detail (or at all). A collection of papers discussing hardware performance can be found on the eSTREAM Web site (Hardware Performance). Also some documents discussing how to evaluate hardware performance can be found. We refer the reader to the Web site for the actual performance result for the different proposals.
Chapter 5

The Next Steps

In March 2006 eSTREAM will announce the details for the Phase II of the project. It is expected that some subset of the submitted proposals will be selected for further analysis, either in the form they were submitted or in a slightly modified (tweaked) form. The details are not finalized.

By necessity, this report is incomplete. Work is currently taking place among a committee of experts from ECRYPT partners and other Virtual Labs to decide on the exact make-up of the eSTREAM second phase.

Steve Babbage VOD Anne Canteaut INRIA Carlos Cid RHUL
Nicolas Courtois AXALTO Henri Gilbert FTRD Thomas Johansson LUND
Joseph Lano KUL Matthew Parker UiB Christof Paar RUB
Bart Preneel KUL Vincent Rijmen GRAZ Matt Robshaw FTRD

It is hoped that the decision on the second phase can be completed by March, 2006. This document is a living one. More information will be added in future updates as the work on eSTREAM continues over the coming years.