eSTREAM - Update 1
September 2, 2005

ECRYPT Network of Excellence

streamciphercall@ecrypt.eu.org

In this update we bring together responses to some of the issues that have arisen during the first few months of eSTREAM. Please feel free to get in touch if you have any queries or comments but, in the meantime, thank you to everyone that has contributed to the project so far.

1 Administration

In this section we deal with some issues of administration[1].

1.1 Project Name and Appropriate Wording

To help with the identification of the project and papers written around this topic, the official name for this ECRYPT managed project will be eSTREAM. We would be grateful if all references in future documentation would use this name. Looking at some of the attention the project is already getting we'd like to emphasize the point that the ECRYPT NoE is not a standardisation body and eSTREAM is not a standardisation effort. To avoid confusion we'd be grateful if references in future documentation could avoid these terms.

Our aim in eSTREAM is to identify a small portfolio of stream ciphers of interest to the community, including standards bodies. While such ciphers won't 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.

1.2 Forum Activity

All interested parties are invited to post comments to the project discussion forum. Like most discussions forums, while it may seem that there is only a "hard core" of people posting, the forum and eSTREAM in general is generating a lot of interest. Web logs reveal that we are averaging around 100 visitors per day with around 500 hits to the eSTREAM pages. With this in mind we encourage everyone to use the discussion forum as much as possible.

[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.

Profile I		*Profile I and II*		*Profile II*	
ABC		F-FCSR		Achterbahn	
CryptMT/Fubuki		Hermes8		DECIM	
DICING		LEX		EDON-80	
DRAGON		MAG		Grain	
Frogbit	A	NLS	A	MICKEY	
HC-256		Phelix	A	MICKEY-128	
Mir-1		Polar Bear		MOSQUITO	
Py		POMARANCH		SFINKS	A
Salsa20		Rabbit		Trivium	
SOSEMANUK		SSS	A	TSC-3	
		TRBDK3 YAEA		VEST	A
		Yamb		WG	
				ZK-Crypt	

Table 1. The submissions to eSTREAM with optional authentication method labelled.

1.3 Workshop Announcement

We are currently planning a two-day workshop towards the end of Phase I. This will allow submitters and analysts to present the latest attacks and developments on eSTREAM submissions as well as other stream cipher issues. Details of the workshop will be announced soon, but we are hoping to hold the workshop during the middle weeks of January 2006 at a convenient European location. More details will become available via `www.ecrypt.eu.org/stream`.

1.4 Moving from Phase I to Phase II

In moving from Phase I to Phase II we feel it is important to reduce the number of submissions by a significant amount. By doing this we can concentrate the efforts of cryptanalysts on a smaller pool of candidates. In moving a candidate submission to Phase II 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
3. Performance when compared to other submissions
4. Justification and supporting analysis
5. Simplicity and flexibility
6. Completeness and clarity of submission

Clearly, submissions with identified security issues cannot be expected to advance. But an algorithm in this unfortunate state might still appear to offer outstanding advantages in other respects. To avoid losing good ideas, it is possible that the submitter of such an algorithm might be invited to try and repair their submission for continued consideration in Phase II. Alternatively, different submitters may see an advantage in combining their approaches. More information on these issues will be made available via `www.ecrypt.eu.org/stream` in the coming months. In the meantime, participants are encouraged to submit useful information about their own or other algorithms either as uploaded documents or as submissions to the discussion forum.

2 Intellectual Property Statements

In Table 2 we list the latest intellectual property conditions of ciphers that were submitted to eSTREAM. We have endeavoured to present the information in a way that is consistent with the information sent to us. If any of the information presented here is not what the submitter intended, please let us know immediately. In the case of every algorithm, any party interested in using an algorithm submitted to eSTREAM should confirm the IPR status directly with the submitter.

3 Security Assessment of Candidates

As is evidenced by the number of paper submissions to eSTREAM and activity on the discussion forum, there has already been considerable cryptanalytic activity. We are grateful for all contributions and encourage this important work to continue. We will collate this information and use it to help move the project forwards to a second phase.

3.1 Withdrawal of Submissions

Some candidates have already received negative cryptanalytic assessment. If a submitter wishes to withdraw an algorithm they are, of course, perfectly at liberty do so. For those algorithms that have received "contentious" analysis we encourage the submitter to make a case for their algorithm, either at the forthcoming workshop, or via the discussion forum, but preferably both.

4 Software Performance Testing

The AES in an appropriate mode is a perfectly adequate stream cipher. Since the security of this solution is not in question, any Profile I submission must demonstrate that it has the potential to outperform the software performance of AES in counter mode. (For those offering an authentication method, a suitable comparison would be to an AES mode that also offers authentication.) With this in mind, we are in the processing of establishing a testing framework (see Section 4.1) that will be used to help move the project forwards to a second phase.

1. Since the results are likely to be academically interesting, we intend to use these tools to measure the software performance of **all** candidate ciphers.

		Algorithm		*Submitted Materials*	
	Profile	*Patent*	*Condition*	*Restriction*	*Condition*
ABC	I	No	-	No	-
Achterbahn	II	No	-	No	-
CryptMT/Fubuki	I	**Yes**	1	**Yes**	1
DECIM	II	**Yes**	3	No	-
DICING	I	No	-	No	4
DRAGON	I	No	-	No	-
EDON-80	II	No	1	No	1
F-FCSR	I + II	No	-	No	-
Frogbit	IA	**Yes**	2	**Yes**	3
Grain	II	No	-	No	4
HC-256	I	No	-	No	-
Hermes8	I + II	No	-	No	4
LEX	I + II	No	-	**Yes**	1
MAG	I + II	No	-	No	-
MICKEY	II	No	-	No	-
MICKEY-128	II	No	-	No	-
Mir-1	I	No	-	No	4
MOSQUITO	II	No	-	No	-
NLS	IA + IIA	No	-	No	-
Phelix	IA + IIA	No	-	No	-
Polar Bear	I + II	No	-	No	-
POMARANCH	I + II	No	-	No	4
Py	I	No	-	No	-
Rabbit	I + II	**Yes**	1	**Yes**	1
Salsa20	I	No	-	No	-
SFINKS	IIA	No	-	No	-
SOSEMANUK	I	No	-	No	-
SSS	IA + IIA	No	-	No	-
TRBDK3 YAEA	I + II	No	1	No	1
Trivium	II	No	-	No	-
TSC-3	II	No	-	No	-
VEST	IIA	**Yes**	3	**Yes**	3
WG	II	No	-	No	-
Yamb	I + II	No	-	No	-
ZK-Crypt	II	**Yes**	1	**Yes**	1

1. Free for non-commercial use, otherwise contact submitter.
2. U.S. restrictions, contact submitter.
3. Contact submitter.
4. If copyrighted material is included in any product, the material must not be covered by licence or patent.

Table 2. The IPR status of submissions to eSTREAM (as of September 2, 2005).

2. **However, the results of this comparison will only be applied to those ciphers that are claimed to be suitable for Profile I.**
3. All submissions to Profile I will be compared with AES-128 in counter mode. Those not passing the performance testing will not be advanced to Phase II.
4. All submissions that are claimed to be suitable for both Profile I and II will be compared with AES-128 in counter mode. Those failing the performance testing can only be advanced to Phase II as a (potential) Profile II cipher.

4.1 Performance Testing Framework

Those that were involved in the AES process will remember that performance testing is a notoriously difficult area. While more details will be made public on `www.ecrypt.eu.org/stream` our initial plans are as follows.

- We will test all submissions on the following platforms:
  32-bit: Intel Pentium 4 and Pentium M; AMD Athlon XP and Sempron.
  64-bit: Alpha; PA-RISC; SPARC; AMD Athlon 64.
- On x86 platforms, the submissions will be compiled with the GNU, Intel, and Microsoft C Compilers, under various compiler options. On the UNIX machines, the testing framework will use the Compaq C compiler, the HP ANSI C Compiler, or the Sun WorkShop Compiler, in addition to the GNU compiler. The fastest implementation (which produces correct test vectors) will be used when comparing the ciphers.
- We will test all submissions with respect to
  - time to encrypt >4 Kbytes measured by encrypting a long stream with calls to the function `ECRYPT_encrypt_blocks()`, and
  - set-up and time to encrypt 40, 576, and 1500 bytes with calls to the function `ECRYPT_encrypt_packet()`.
- Note that the `ECRYPT_encrypt_packet()` function includes the IV initialisation (and the MAC finalisation for authenticating stream ciphers), but no key setup. The time taken by the latter will be measured separately.
- Any cipher that we cannot test will not be advanced to Phase II.
- We positively welcome and encourage any third-party assessments.

We realise that many submitters have sent reference (i.e. unoptimised) code during the call for submissions. For this reason submitters can, if they like, submit optimised code by December 2, 2005. However, please note the following points:

1. **Please do not send code now.** We will announce details on the submission of optimised code on `www.ecrypt.eu.org/stream`.
2. We will use the code that accompanied the submission as a default.
3. We have already tested the submitted code and the results will be announced on `www.ecrypt.eu.org/stream`.
4. If, as a submitter, you are happy with the performance of your submitted code then this is the code we will use for performance testing.

5. We will test the most recent, single version of the code that is available to us on December 2, 2005.

An assessment of the suitability of the different ciphers with respect to different criteria will not be straightforward. In particular, some ciphers may attain a fast performance at the expense of constructing large tables during the initialisation phase. We intend to take these issues into account and aim to use the results of performance testing to reveal an array of broad trade-offs and trends.

5 Hardware Performance Testing

Since the AES in an appropriate mode is a perfectly adequate stream cipher this will be our benchmark for comparison. In fact, in some sense we have already given an advantage to Profile II submissions since these submissions need only provide a security level of 2^{80} (rather than the 128 bits provided by the AES).

Given the difficulty in making hardware-related performance estimates (either in terms of speed, power, or area) we have not yet established a testing framework for Profile II candidates. We have however been in touch with ECRYPT institutions within the VAMPIRE Virtual Lab (which covers *implementation issues*) and we already have several initiatives in hand. We anticipate hardware performance to be a main consideration in Phase II. More details will become available on `www.ecrypt.eu.org/stream`. Of course, we welcome any third party analysis and contributions on this issue.

6 Feedback and Comments

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