# The eSTREAM Portfolio

Steve Babbage[1], Christophe De Cannière[2,3], Anne Canteaut[4], Carlos Cid[5], Henri Gilbert[6], Thomas Johansson[7], Matthew Parker[8], Bart Preneel[2], Vincent Rijmen[2,9], and Matthew Robshaw[6]

[1] Vodafone, United Kingdom
[2] COSIC and IBBT, K.U.Leuven, Belgium
[3] École Normale Supérieure, France
[4] INRIA, France
[5] Royal Holloway, United Kingdom
[6] Orange Labs, France
[7] University of Lund, Sweden
[8] Selmer Centre, University of Bergen, Norway
[9] T.U. Graz, Austria

April 15, 2008

This work has been supported by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. 

## 1 Introduction

After more than three years eSTREAM has come to an end. In this note we describe the final "portfolio" which contains what we believe to be the more successful eSTREAM submissions and we highlight some areas of open research.

The goal of eSTREAM was to stimulate work in the area of stream ciphers. In this, undoubtedly, the project has been a success. While eSTREAM has much of the appearance of a competition such as that used to establish the AES (or the forthcoming SHA-3) this comparison should be resisted. We prefer not to use the word "winners", or to necessarily pick one (or even two) algorithms as the sole outcome of eSTREAM. Rather, we are conscious that most of the stream ciphers in the portfolio are very new and while we believe them to be promising—for a variety of reasons—we must leave it to others to decide when analysis is sufficiently mature for an algorithm to be considered in standards or used in a deployment. In fact, due to the immature nature of most eSTREAM algorithms and the research-oriented agenda of eSTREAM, the portfolio we have arrived at might be broader than some would have expected. However, by highlighting a broader pool of stream ciphers we believe that we are offering a better choice of options in meeting different performance requirements and security margins. And by promoting a portfolio that reflects the remarkable diversity of design approaches, we believe that we are giving the cryptographic community every chance to continue building its know-how in stream cipher design and analysis.

## 2 eSTREAM Portfolio

Our portfolio contains the following algorithms (in alphabetical order).

| *Profile 1* | *Profile 2* |
|---|---|
| HC-128 | F-FCSR-H v2 |
| Rabbit | Grain v1 |
| Salsa20/12 | MICKEY v2 |
| Sosemanuk | Trivium |

In the sections that follow we give a brief summary of our views on each of the eSTREAM finalists in turn. While we have used all the information at hand in making our decisions, one of the purposes of eSTREAM was to promote developments in stream cipher design and analysis. As a consequence we view the portfolio as being a snap-shot of a fast-moving field. All the designs in the eSTREAM portfolio are relatively immature and it is possible that more analysis will change the picture dramatically. With this in mind, we intend to maintain the eSTREAM web-pages for the foreseeable future and to update the portfolio as circumstances dictate.

## 3 The Profile 1 (Software-oriented) Finalists

The goal for ciphers submitted to Profile 1 was that they should be "good" in software. By this we meant that they should significantly outperform the AES when used in a suitable stream cipher mode and all the final phase ciphers in Profile 1 achieve this.

Our vision wasn't necessarily of a stream cipher that had a good all-round profile; our focus was on raw encryption speed with a bias towards encrypting large amounts of data after a single initialisation. Our intended security level was set to 128 bits which we believe to be adequate for contemporary applications.

While such properties were intended to give the designer enough design-space to really achieve something outstanding, we are also pragmatic. There may well be applications that demand frequent re-keying or re-initialisation, and some users may prefer a security level of 256 bits. And while the eSTREAM project has attempted to remain agnostic with regards to the issue of intellectual property, we know significant sectors of the community are strongly adverse to algorithms that are restricted in this way. We have therefore tried to keep all these aspects in mind in arriving at the broad mix of algorithms that constitute our portfolio for Profile 1.

**CryptMT v3.** The cipher CryptMT has a very unusual design which delivers very reasonable performance. While there have been no negative cryptanalytic results against the cipher in the last phase of eSTREAM, we are somewhat concerned that the security of the cipher, in particular the non-linear filter component, might not yet be as well-understood as some of the other finalists. We anticipate that elements of CryptMT will continue to be of interest to the cryptographic community, and we hope that the full advantages of the approach embodied in CryptMT v3 can be evaluated. However, we are currently not sufficiently confident in the design and security of this algorithm for us to include it in the final portfolio.

**Dragon.** The Dragon cipher appears to be of solid construction. It is attractive enough to have received considerable cryptanalytic attention over the course of eSTREAM, and it has resisted all attacks that have so far been described against the cipher (with some margin to spare). Since it also compares reasonably well to AES in counter mode, the stated aim of eSTREAM, it should be considered a highly successful design. The downside to the current design of Dragon, is that while its performance is competitive with the AES, it does not compare too well to the other submissions in the final phase. It would certainly be interesting if a future version of the cipher were able to maintain some of the successful design ideas while delivering even better performance.

**HC-128.** In many ways HC-128 is the best match for the initial intended goals of eSTREAM. It offers very impressive performance in software applications where

we wish to encrypt large streams of data. HC-128 is a variant of the original HC-256 [12], and hence the cipher is perhaps not yet as established as some of the other eSTREAM candidates. Still, despite the design's high profile, there have been no cryptanalytic advances against it, and we have no indication that the security margin is at all tight. We believe that the impressive raw encryption speed of HC-128 makes it a particularly interesting proposal. However, since HC-128 is table-driven there is a cost in the time to initialise the cipher. Thus, for applications that might want to re-initialise often, there can be a significant performance penalty that some might prefer to avoid. This is particularly evident in the original 256-bit version. HC-128 appears to be a very strong performer for link-level streamed applications, but a relatively poor performer for typical packetised applications. For such applications, the eSTREAM portfolio supports alternatives to HC-128 that offer a better-balanced performance profile.

**LEX v2.** As one of the most elegant (and provocative!) designs in eSTREAM, LEX scores many considerable successes. Built on the AES, LEX can directly leverage much of the implementation and analytic know-how behind this trusted cipher. In terms of a fully defined submission to eSTREAM and in comparison to the other finalists, however, we are somewhat wary and this is a view that appears, at least to some degree, to be reflected in the voting at SASC 2008 (see Section 5). While they might not be necessarily threatening, there are structural features [7] in LEX that are not apparent in the other submissions. Further, LEX carries the most restrictive usage requirements of all the finalists. While the performance of LEX is reasonable (the submitted code is not particularly competitive but some improved results are available independently [1]) there are some very recent cryptanalytic results on the cipher [4]. We finally decided not to include LEX v2 in the final portfolio. However we encourage others to work with the LEX philosophy, to develop it, and to gauge the full extent and true security picture of such a cipher design for the future.

**NLS v2.** In Phase 3 of eSTREAM we considered only the NLSv2 cipher, not the associated MAC function that was part of the original design. While a broadly successful cipher design, we felt that NLS v2 didn't quite keep up with the other algorithms in the portfolio. In terms of performance, it almost consistently out-performs the AES in counter mode, successfully accomplishing one of the primary goals of eSTREAM. However its performance when compared to the other finalists was less successful. In addition, it wasn't clear that there was a substantial margin for security. Distinguishers for NLS v2 have been claimed that require enormous amounts of plaintext; while they can be considered impractical they do appear to undercut the stated security goal of the cipher. We feel it would be interesting if the designers were able to re-use some of the nice performance elements from NLS v2 in future work.

**Rabbit.** From among the eSTREAM submissions, Rabbit is one of the oldest designs and has remained unchanged since its publication at FSE 2003 [3]. In

the absence of cryptanalytic results against the cipher this is clearly a positive sign. Added to this, the cipher appears to offer a broad and pleasing performance profile, with some recently submitted code being particularly well-suited to newer Intel processors. We feel that this algorithm complements HC-128 well. Some commentators might dislike the lack of support for longer key lengths, or the existence of intellectual property on the cipher. However, for the purposes of eSTREAM, our goal was an algorithm that offered 128-bit security, and we set IP issues to one side. It is for those who wish to use the ciphers to choose the factors that matter in their circumstances, and to make their choices accordingly.

**Salsa20/12.** This cipher offers a simple, clean, and scaleable design. As well as supporting 128-bit and 256-bit keys in a very natural way, the simplicity and scalability of the algorithm has undoubtedly contributed to it receiving much cryptanalytic attention. For our portfolio we propose a version of Salsa20 that has twelve rounds. Eight and twenty round versions were also considered during the eSTREAM process, but we feel that Salsa20/12 offers the best balance, combining a very nice performance profile with what appears to be a comfortable margin for security. In our view Salsa20/12 is a very successful proposal.

**Sosemanuk.** All the available information on Sosemanuk suggests that the cipher offers a very considerable margin for security. Yet, at the same time, the performance profile demonstrates that the cipher delivers very reasonable trade-offs. The overt re-use of components from earlier block cipher designs is an interesting idea and we suspect that the cipher will remain of considerable research interest. In our view Sosemanuk makes a good complement to the other software-oriented ciphers in the portfolio and this appears to be a broadly held view, as evidenced by the voting at SASC 2008 (see Section 5).

## 4 The Profile 2 (Hardware-oriented) Finalists

The goal for ciphers submitted to Profile 2 was that they should be "good" in constrained hardware environments. By this we meant that ciphers should significantly out-perform the AES in a restricted environment in at least one significant regard. The final phase candidates in Profile 2 were chosen because we believed they had the potential to achieve this.

We were anticipating that ciphers in Profile 2 might be suitable for deployment on passive RFID tags or low-cost devices such as might be used in sensor networks. Such devices are exceptionally constrained in computing potential because of the number of logic gates available or the amount of power that might realistically be available. Our intended security level for this profile was 80 bits which we believe to be adequate for the lower-security applications where such devices might be used. Some companion algorithms supporting 128 bits of security have been proposed. While these are not directly included in the portfolio, they remain of considerable interest.

**Decim v2.** Decim contains a unique component in eSTREAM, that of irregular decimation, and is an interesting addition to the field of stream ciphers. While the first version did not fare too well, the major re-design that followed has seemingly led to a much stronger version, for which no adverse cryptanalytic results are known. That said, the cipher doesn't seem to deliver such a satisfying performance profile, so while there might be some very interesting elements to the Decim construction, we feel that the current proposal doesn't compare too well to the other submissions for the hardware profile.

**Edon-80.** This is one of the more original algorithms that was submitted to eSTREAM. The designers are to be congratulated for trying a different design element that has been, for the most part, highly successful. There have been no catastrophic breaks of Edon-80. There are, however, some cryptanalytic results [5] that demonstrate a slight erosion to a very high security level though the designers of Edon-80 discussed this conclusion at SASC 2008. Our decision not to include Edon-80 in the final portfolio is, rather, a reflection of the performance offered by the algorithm. While its presence as a finalist reflects our belief that it will outperform the AES in a restricted hardware environment in at least one significant regard, we fear that Edon-80 is, in turn, outperformed by the ciphers in the final portfolio.

**F-FCSR-H v2.** Related to foundational work in the mid-1990's, notably that of Klapper and Goresky, this cipher embodies a simple but seemingly effective approach. While it is not as versatile in implementation as Grain v1 or Trivium, it tends to lie in the top half of most hardware performance classifications. In our view, the lack of results against the cipher and the very reasonable performance profile make F-FCSR-H an interesting representive from a long-standing area of stream cipher research. This, in turn, makes the cipher a welcome addition to the portfolio.

**Grain v1.** One of the simplest designs in eSTREAM, Grain v1 is an algorithm that has pushed the state of the art in terms of compact implementation. The simplicity and high profile of the design has meant that the cipher has come under much scrutiny, and this has indicated that the security margin is, in truth, very tight. Nevertheless, the cipher is attractive and well-suited for compact implementations, and its pipelining capabilities offer valuable flexibility to the implementer. Grain v1 is therefore a worthy member of the hardware portfolio. For further research however, particularly if there is an eye towards eventual implementation of the algorithm, we hope that the designers will consider all the recent cryptanalytic work and ideally propose a future version of Grain that replaces the current initialisation phase.

**MICKEY v2.** According to most performance metrics MICKEY v2 tucks in behind Grain v1 and Trivium. While it doesn't offer the same implementation

flexibility as the two latter algorithms, the designers have seemingly made some conservative choices. While there are some risks that a conservative approach could lead to a complicated design, this is not the case for MICKEY v2. The clarity and simplicity of the cipher has been commented on [9] and this is a positive attribute. There have been no negative cryptanalytic results against the cipher and we believe that it is likely to be of future research interest.

**Moustique.** As the only self-synchronising cipher left in eSTREAM, Moustique is particularly noteworthy. The unusual features of this kind of stream cipher are well-known and the security demands they place on a design are significant. Unfortunately cryptanalysis [10] has revealed some undesirable attributes to the cipher and it seems that the design might not be as robust as we might ideally like. That said the design of a self-synchronising stream cipher is a noteworthy challenge and we look forward to seeing a new version of the cipher, or a close relative, in the near future.

**Pomaranch v3.** Like all the ciphers in Phase 3, Pomaranch is a notable design. However, somewhat like Edon-80, it has not been as successful as some other submissions when looked at in detail. While there have been some cryptanalytic results against the cipher [6], they lie at the fringes of the security limits and their implications are open to some discussion. Instead, our decision not to include Pomaranch v3 in the final portfolio is more a reflection on the performance of the algorithm. Unfortunately, in a field of very strong proposals, the cipher doesn't seem to compete too well with the other options available.

**Trivium.** This algorithm leads the field in many respects. Simple and clean in design, the clarity of the cipher has inspired many to attempt to cryptanalyse it. Yet, at the time of writing, there are no results against the cipher. Added to this we have an exceptional performance profile in hardware (which is even coupled with a strong performance profile in software). Trivium appears to be a very good match for the goals of eSTREAM. Some commentators are a little wary of the exceptional simplicity of Trivium and this is not without some justification. Thus we feel, as for all new ciphers in eSTREAM, that it may be prudent to wait a little longer to be sure that any ongoing security analysis has reached sufficient maturity. Nevertheless, from our current vantage point, Trivium appears to be a highly successful design, a view that is shared with the attendees at SASC 2008.

## 5 Voting at SASC 2008

We were not bound by the results of voting at SASC 2008 and we feel such votes should only be viewed as indicative. However the trends that appear might still be of some interest. Since our own technical assessment was independent of the voting results, it was pleasing to see such a close match with our own views. While we might have chosen to put some of the portfolio algorithms in a different order

(if we had chosen to provide an ordering), the actual contents of the portfolio are a direct match with the general views expressed at SASC 2008.

For each algorithm attendees were asked to tick one of the following three choices regarding its suitability for the final portfolio: *very suitable*, *neutral*, *not very suitable*. The first and third votes counted for +5 and -5 points each, with the final score being averaged over the number of votes cast for a given algorithm.

| | | | | |
|---|---|---|---|---|
| Rabbit | 2.80 | | Trivium | 4.35 |
| Salsa20 | 2.80 | | Grain v1 | 3.50 |
| Sosemanuk | 1.20 | | F-FCSR-H v2 | 0.52 |
| HC-128 | 0.60 | | MICKEY v2 | 0.17 |
| NLS v2 | -0.60 | | Decim v2 | -1.38 |
| LEX v2 | -1.20 | | Edon80 | -1.72 |
| CryptMT v3 | -1.40 | | Pomaranch v3 | -2.24 |
| Dragon | -1.60 | | Moustique | -2.50 |

It is interesting to note the strong views expressed for the hardware ciphers, with the software ciphers being somewhat harder to separate.

## 6 Some Open Issues

While providing a very significant body of new work that advances the field, the eSTREAM project also confirmed some of the more difficult problem areas in stream cipher work.

Certainly it seems to be difficult to design self-synchronising stream ciphers. Very few self-synchronising proposals were submitted to eSTREAM; those that were illustrated the difficulties that could be encountered. This appears to be a very significant open problem and we encourage designers to consider this issue as an active area of research. A second area that appeared to cause some difficulties was that of adding some mechanism for authentication to a stream cipher. Given the properties of stream cipher encryption this would be a very desirable attribute, and yet the final portfolio suggests that an appropriate way to do this still remains undiscovered.

On the cryptanalytic side, we have been intrigued by the developing work on the initialisation of stream ciphers by several different groups of researchers, and in particular its application to the hardware-oriented ciphers where designers have been working in an environment where significant margins of security are a luxury. The cryptanalytic work, while increasingly effective, is acknowledged by some of the cryptanalysts themselves as being somewhat *ad hoc*. This is, therefore, a pressing area of stream cipher analysis and, as an anticipated consequence, of future stream cipher designs.

Looking to the future, we expect research to continue on all the eSTREAM submissions and not just the portfolio ciphers. In fact we recommend ongoing analysis of stream ciphers in general. For instance, even though SNOW 2.0 [8] was not submitted we believe that it would make a perfect accompaniment to the Profile 1 (software-oriented) portfolio ciphers. We would also like to emphasize

that the earlier stages of eSTREAM included many innovative designs such as the TPy family [2] and Phelix [11]. We believe that these are still of considerable interest and, independently of the long-term status of the portfolio ciphers, we believe that there still remains room for new and provocative stream cipher designs.

## 7 Conclusions

Q: *Stream ciphers: dead or alive?*

A: Over the course of eSTREAM the cryptographic community has studied 34 stream ciphers and their tweaked versions. Ciphers were submitted from around the world and the project web-pages received tens of thousands of distinct visitors each year of the project. In terms of research, our greater understanding of stream cipher design and cryptanalysis is reflected by a wide range of papers in recent conference proceedings and journals. All this has led to some very promising new proposals. At the first SASC workshop, Adi Shamir suggested that any future for dedicated stream ciphers would probably lie in extreme software speed or in restricted hardware implementation. With the eSTREAM portfolio we hope to confirm this intuition and we propose candidate algorithms for both scenarios. Along the way we have seen that stream cipher design is not easy, but everyone who submitted to eSTREAM was willing to take on the challenge and we thank them all for their innovative and impressive work.

## References


1. D. Bernstein. Which phase-3 eSTREAM ciphers provide the best software speeds? Available via `cr.yp.to/streamciphers/phase3speed-20080331.pdf`.
2. E. Biham and J. Seberry. Tweaking the IV Setup of the Py Family of Stream Ciphers—The Ciphers TPy, TPypy, and TPy6. Paper 2007/038 at `www.ecrypt.eu.org/stream/papers.html`.
3. M. Boesgaard, M. Vesterager, T. Pedersen and O. Scavenius. Rabbit: A New High-Performance Stream Cipher. In T. Johansson, editor, *Proceedings of FSE 2003*, Lecture Notes in Computer Science, volume 2887, pages 226–244, Springer, 2004.
4. O. Dunkelman and N. Keller. A New Attack on the LEX Stream Cipher. Preprint.
5. M. Hell and T. Johansson. A Key Recovery Attack on Edon80. In K. Kurasawa, editor, *Proceedings of Asiacrypt 2007*, Lecture Notes in Computer Science, volume 4833, pages 568–581, Springer, 2007.
6. H. Englund, M. Hell, and T. Johansson. Two General Attacks on Pomaranch-like Keystream Generators. In A. Biryukov, editor, *Proceedings of FSE 2007*, Lecture Notes in Computer Science, volume 4593, pages 274–289, Springer, 2007.
7. H. Englund, M. Hell, and T. Johansson. A Note on Distinguishing Attacks. Paper 2007/013 at `www.ecrypt.eu.org/stream/papers.html`.
8. H. Englund and T. Johansson. A New Version of the Stream Cipher Snow. In K. Nyberg and H. Heyes, editors, *Proceedings of SASC 2002*, Lecture Notes in Computer Science, volume 2595, pages 47–61, Springer, 2003.

9. T. Good and M. Benaissa. Hardware Performance of eSTREAM Phase III Stream Cipher Candidates. In *Workshop record for SASC 2008*, available via `http://www.ecrypt.eu.org/stvl/sasc2008`.
10. E. Kasper, V. Rijmen, T. Bjorstad, C. Rechberger, M. Robshaw, and G. Sekar. Correlated Keystreams in Moustique. In S. Vaudenay, editor, *Proceedings of Africacrypt 2008*, Lecture Notes in Computer Science, Springer. To appear.
11. D. Whiting, B. Schneier, S. Lucks and F. Muller. Phelix—Fast Encryption and Authentication in a Single Cryptographic Primitive. Paper 2005/020 at `www.ecrypt.eu.org/stream/papers.html`.
12. H. Wu. A New Stream Cipher HC-256. In B. Roy and W. Meier, editors, *Proceedings of FSE 2004*, Lecture Notes in Computer Science, volume 3017, pages 226–244, Springer, 2004.