The eSTREAM Portfolio (rev. 1)

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, K.U.Leuven and IBBT, 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

September 8, 2008

The eSTREAM portfolio was published in April 2008 [2] with the opinion that

> [. . .] 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.

Following the publication of cryptanalytic results [3] against F-FCSR-H v2 [1], we have decided to make our first revision to the portfolio. While F-FCSR-H v2 embodied a simple design with interesting cipher characteristics, refined analysis has found this particular design to be flawed. We have therefore decided to revise the portfolio which now contains the following algorithms (in alphabetical order).

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

The stream ciphers in the revised portfolio (to be denoted by *rev. 1*) are still very new and we leave it to others to decide when analysis is sufficiently mature for an algorithm to be considered in standards or in a deployment.

References

1. F. Arnault, T. Berger, and C. Lauradoux. F-FCSR Stream Ciphers. In M.J.B. Robshaw and O. Billet, editors, New Stream Cipher Designs: The eSTREAM Finalists, volume 4986 of Lecture Notes in Computer Science, pages 170–178, Springer, 2008. Also available via `http://www.ecrypt.eu.org/stvl/`.
2. S. Babbage, C. De Cannière, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M.J.B. Robshaw. The eSTREAM Portfolio. Available via `http://www.ecrypt.eu.org/stvl/`.
3. M. Hell and T. Johansson. Breaking the F-FCSR-H stream cipher in Real Time. In J. Pieprzyk, editor, *Proceedings of Asiacrypt 2008*, Lecture Notes in Computer Science, to appear.