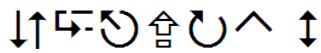


ECRYPT II



ICT-2007-216676

ECRYPT II

European Network of Excellence in Cryptology II

Network of Excellence

Information and Communication Technologies

D.SYM.3

The eSTREAM Portfolio 2009 Annual Update

Due date of deliverable: 31. July 2009

Actual submission date: 01. October 2009

Start date of project: 1 August 2008

Duration: 4 years

Lead contractor: Royal Holloway (RHUL)

Revision 1.1

Project co-funded by the European Commission within the 7th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

The eSTREAM Portfolio

2009 Annual Update

Editors

Carlos Cid (RHUL) and Matthew Robshaw (FT)

01. October 2009

Revision 1.1

The work described in this report has in part been supported by the Commission of the European Communities through the ICT program under contract ICT-2007-216676. 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	The eSTREAM Portfolio – 2009 Annual Update	1
1.1	Introduction	1
1.2	Cryptanalytic Results	2
1.3	Implementation Results	2
1.4	Other Developments	2

Chapter 1

The eSTREAM Portfolio – 2009 Annual Update

1.1 Introduction

eSTREAM, a multi-year project co-ordinated by ECRYPT, came to an end in 2008. The eSTREAM project finished with the publication of a portfolio of promising new stream ciphers that might be suited to fast encryption in software (Profile 1) or efficient encryption—in terms of physical resources—in hardware (Profile 2). The final portfolio, published in April 2008, contained eight algorithms [5]. The portfolio was revised in September 2008 [6] after the announcement of cryptanalytic results against one of the algorithms [16]. The current eSTREAM portfolio contains the following seven algorithms (in alphabetical order).

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

When the portfolio was published [5, 6], it was the opinion of the eSTREAM committee that all the algorithms in the portfolio were relatively immature. And even though confidence in the portfolio ciphers will increase over time, this still remains the considered position of experts in the field. With this in mind, the portfolio is periodically revisited with an eye to any new results in the literature.

In this report we highlight some cryptanalytic results that have helped increase our understanding of the portfolio ciphers, along with results that might signal structural features impacting their practical use and deployment. We also mention new results on the hardware and/or software implementation of portfolio ciphers that may be of interest to developers seeking to implement the stream ciphers. However, even after a year of additional research, the eSTREAM portfolio remains unchanged. So while the portfolio algorithms will certainly benefit from more analysis over coming years, at the moment their design still appears to

be sound. eSTREAM continues to be maintained and any changes to the portfolio will be announced on <http://www.ecrypt.eu.org/stream/>.

1.2 Cryptanalytic Results

It is gratifying that analysis of the portfolio algorithms has continued beyond the publication of the portfolio and the end of the eSTREAM project. As well as a brief survey of the literature we have consulted the algorithm designers and there appear to be no new results that question the security claims of the portfolio ciphers.

For instance, there are a few publications analysing features of the Salsa20 family of stream ciphers [2, 17, 22], but these do not seem to affect the security of the Salsa20/12 algorithm [8] itself. Likewise, recent analysis of HC-128 [21], Rabbit [20], and Sosemanuk [19] do not affect the practical security of these ciphers.

For the hardware-oriented ciphers (Profile 2), while some articles have discussed generic stream cipher properties and used MICKEY as the focus of their analysis [1, 23], there appear to be no new security results on MICKEY v2. The initialisation of both Trivium and Grain v1 continues to interest cryptanalysts [24, 10, 3, 4, 12] and while notable progress has been made in the analysis of this component, the status of these algorithms remains unchanged from last year.

1.3 Implementation Results

The best references for implementation profile of eSTREAM algorithms in hardware are [11, 13, 14, 18, 15], some of which appeared before the publication of the eSTREAM portfolio. The software performance of the eSTREAM ciphers was presented in [9] with further extensive results being available at [7].

1.4 Other Developments

There have been some other developments with the portfolio ciphers that may be of interest to the community. Rabbit has been released into the public domain and the designers confirm that it can be used freely for any purpose. We also note that CyaSSL [25], an open source embedded implementation of the SSL/TLS protocol, includes both HC-128 and Rabbit in their latest release version.

Bibliography

- [1] M. Afzal and A. Masood. Resistance of Stream Ciphers to Algebraic Recovery of Internal Secret States. *Third International Conference on Convergence and Hybrid Information Technology, ICCIT*, vol. 2, pp. 625–630, 2008.
- [2] J-P. Aumasson, S. Fischer, S. Khazaei, W. Meier and C. Rechberger. New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba. In K. Nyberg, editor, *Proceedings of FSE 2008*, LNCS 5086, pp. 470–488, Springer 2008.
- [3] J-P. Aumasson, I. Dinur, W. Meier and A. Shamir. Cube testers and key recovery attacks on reduced-round MD6 and Trivium. In O. Dunkelman, editor, *Proceedings of FSE 2009*, LNCS 5665, pp. 1–22, Springer, 2009.
- [4] J-P. Aumasson, I. Dinur, L. Henzen, W. Meier and A. Shamir. Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128. *Cryptology ePrint Archive*, Report 2009/218. <http://eprint.iacr.org/2009/218>.
- [5] 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. April 2008. Available via <http://www.ecrypt.eu.org/stream/>.
- [6] 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 (rev. 1). September 2008. Available via <http://www.ecrypt.eu.org/stream/>.
- [7] D.J. Bernstein. Notes on the ECRYPT Stream Cipher project (eSTREAM). <http://cr.yp.to/streamciphers.html>.
- [8] D.J. Bernstein. Salsa20 page. <http://cr.yp.to/snuffle.html>.
- [9] C. De Cannière. eSTREAM Software Performance. In M. Robshaw and O. Billet, editors. *New Stream Cipher Designs: The eSTREAM Finalists*. LNCS 4986, pp. 119–139. Springer 2008.
- [10] I. Dinur and A. Shamir. Cube Attacks on Tweakable Black Box Polynomials. In A. Joux, editor, *Advances in Cryptology - EUROCRYPT 2009*, LNCS 5479, pp. 278–299, Springer 2009.
- [11] K. Gaj, G. Southern, and R. Bachimanchi. Comparison of Hardware Performance of Selected Phase II eSTREAM Candidates. In *Proceedings of SASC 2007*, Bochum, 2007. Workshop record available via <http://www.ecrypt.eu.org/stream/>.

- [12] S. Fischer, S. Khazaei and W. Meier. Chosen IV Statistical Analysis for Key Recovery Attacks on Stream Ciphers. In S. Vaudenay, editor, *Proceedings of AFRICACRYPT 2008*, LNCS 5023, pp. 236–245, Springer 2008.
- [13] T. Good and M. Benaïssa. Hardware results for selected stream cipher candidates. In *Proceedings of SASC 2007*, Bochum, 2007. Workshop record available via <http://www.ecrypt.eu.org/stream/>.
- [14] T. Good and M. Benaïssa. Hardware performance of eStream phase-III stream cipher candidates. In *Proceedings of SASC 2008*, Lausanne, 2008. Workshop record available via <http://www.ecrypt.eu.org/stream/>.
- [15] T. Good and M. Benaïssa. ASIC Hardware Performance. In M. Robshaw and O. Billet, editors. *New Stream Cipher Designs: The eSTREAM Finalists*. LNCS 4986, pp. 267–293. Springer 2008.
- [16] M. Hell and T. Johansson. Breaking the F-FCSR-H stream cipher in Real Time. In J. Pieprzyk, editor, *Proceedings of Asiacrypt 2008*, LNCS 5350, pp. 557–569, Springer 2008.
- [17] J.C. Hernandez-Castro, J. M. E. Tapiador, J.-J. Quisquater. On the Salsa20 Core Function. In K. Nyberg, editor, *Proceedings of FSE 2008*, LNCS 5086, pp. 462–469, Springer 2008.
- [18] D. Hwang, M. Chaney, S. Karanam, N. Ton, and K. Gaj. Comparison of FPGA-Targeted Hardware Implementations of eSTREAM Stream Cipher Candidates. In *Proceedings of SASC 2008*, Lausanne, 2008. Workshop record available via <http://www.ecrypt.eu.org/stream/>.
- [19] J.-K. Lee, D.H. Lee and S. Park. Cryptanalysis of Sosemanuk and SNOW 2.0 Using Linear Masks. In J. Pieprzyk, editor, *Proceedings of Asiacrypt 2008*, LNCS 5350, pp. 524–538, Springer 2008.
- [20] Y. Lu, H. Wang and S. Ling. Cryptanalysis of Rabbit. In T.-C. Wu et al, editors, *Proceedings of ISC 2008*. LNCS 5222, pp. 204–214, Springer 2008.
- [21] S. Maitra, G. Paul and S. Raizada. Some Observations on HC-128. *Proceedings of the International Workshop on Coding and Cryptography (WCC)*, May 10-15, 2009, Ullensvang, Norway, pp. 527–539.
- [22] D. Priemuth-Schmid and A. Biryukov. Slid Pairs in Salsa20 and Trivium. In D.R. Chowdhury, V. Rijmen, and A. Das, editors, *Progress in Cryptology - INDOCRYPT 2008*, LNCS 5365, pp. 1–14, Springer 2008.
- [23] A. Röck. Stream Ciphers Using a Random Update Function: Study of the Entropy of the Inner State. In S. Vaudenay, editor, *Proceedings of AFRICACRYPT 2008*, LNCS 5023, pp. 258–275, Springer 2008.
- [24] M. Vielhaber. Breaking ONE.FIVIUM by AIDA an Algebraic IV Differential Attack. Cryptology ePrint Archive, Report 2007/413. <http://eprint.iacr.org/2007/413>.
- [25] yaSSL. Yet Another SSL. Available via www.yassl.com.