

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Matthew Robshaw Olivier Billet (Eds.)

New Stream Cipher Designs

The eSTREAM Finalists

Volume Editors

Matthew Robshaw

Olivier Billet

Orange Labs

38–40 rue du Général Leclerc, 92794 Issy-les-Moulineaux CEDEX 9, France

E-mail: {matt.robshaw, olivier.billet}@orange-ftgroup.com

Library of Congress Control Number: 2008927529

CR Subject Classification (1998): E.3, F.2.1-2, G.2.1, D.4.6, K.6.5, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-68350-X Springer Berlin Heidelberg New York

ISBN-13 978-3-540-68350-6 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2008

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12273416 06/3180 5 4 3 2 1 0

Preface

The question “Stream ciphers: dead or alive?” was posed by Adi Shamir. Intended to provoke debate, the question could not have been better, or more starkly, put. However, it was not Shamir’s intention to suggest that stream ciphers themselves were obsolete; rather he was questioning whether stream ciphers of a *dedicated design* were relevant now that the AES is pervasively deployed and can be used as a perfectly acceptable stream cipher.

To explore this question the *eSTREAM Project* was launched in 2004, part of the EU-sponsored ECRYPT Framework VI Network of Excellence. The goal of the project was to encourage academia and industry to consider the “dead stream cipher” and to explore what could be achieved with a dedicated design. Now, after several years of hard work, the project has come to a close and the 16 ciphers in the final phase of eSTREAM are the subject of this book.

The designers of all the finalist ciphers are to be congratulated. Regardless of whether a particular algorithm appears in the final portfolio, in reaching the third phase of eSTREAM all the algorithms constitute a significant milestone in the development of stream ciphers.

However, in addition to thanking all designers, implementers, and cryptanalysts who participated in eSTREAM, this is a fitting place to offer thanks to some specific individuals.

The international and collaborative nature of the project was only possible with a good supporting infrastructure and many thanks are due to Joe Lano who got eSTREAM off to such a good start. His role was passed to Hongjun Wu and then to Orr Dunkelman, who both kept things moving seamlessly. Many experts dedicated their time by serving on the eSTREAM internal evaluation committee. Together they have helped the project navigate its way through some very difficult and sensitive decisions:

Steve Babbage	Vodafone, UK
Christophe De Cannière	K.U.Leuven, Belgium and ENS, France
Anne Canteaut	INRIA, France
Carlos Cid	Royal Holloway, UK
Henri Gilbert	Orange Labs, France
Thomas Johansson	University of Lund, Sweden
Joe Lano	K.U.Leuven, Belgium
Christof Paar	University of Bochum, Germany
Matthew Parker	University of Bergen, Norway
Bart Preneel	K.U.Leuven, Belgium
Vincent Rijmen	K.U.Leuven, Belgium and T.U. Graz, Austria
Hongjun Wu	K.U.Leuven, Belgium

The eSTREAM project depended on events and workshops so that ideas could be presented and debated. These were, without exception, highly successful and

for their help as General or Program Chairs, or in chairing discussions, special thanks are extended to Steve Babbage, Christophe De Cannière, Anne Canteaut, Orr Dunkelman, Thomas Johansson, Lars Knudsen, Joe Lano, Kerstin Lemke-Rust, and Bart Preneel. Throughout, the administrative support extended by K.U.Leuven was outstanding and special thanks are due to Péla Noë.

Finally, the most important contributors to eSTREAM have been all the cipher designers, the implementers, and the analysts. We are very grateful for all the work that went into preparing a submission and to all those who crypt-analyzed, implemented, and commented on the candidates. While some will be disappointed that their algorithm was not advanced from the earlier stages of eSTREAM or that it is not included in the final portfolio, we would like to acknowledge all the contributions made to eSTREAM and to thank all submitters for collectively advancing the field of stream ciphers by a very significant margin.

April 2008

M.J.B. Robshaw

This work has been supported by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document 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 its sole risk and liability.

Table of Contents

The eSTREAM Project	1
<i>Matthew Robshaw</i>	
CryptMT3 Stream Cipher	7
<i>Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita</i>	
The Dragon Stream Cipher: Design, Analysis and Implementation Issues	20
<i>Ed Dawson, Matt Henricksen, and Leonie Simpson</i>	
The Stream Cipher HC-128	39
<i>Hongjun Wu</i>	
Design of a New Stream Cipher—LEX	48
<i>Alex Biryukov</i>	
Specification for NLSv2	57
<i>Philip Hawkes, Cameron McDonald, Michael Paddon, Gregory G. Rose, and Miriam Wiggers de Vries</i>	
The Rabbit Stream Cipher	69
<i>Martin Boesgaard, Mette Vesterager, and Erik Zenner</i>	
The Salsa20 Family of Stream Ciphers	84
<i>Daniel J. Bernstein</i>	
SOSEMANUK, a Fast Software-Oriented Stream Cipher	98
<i>Côme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, and Hervé Sibert</i>	
eSTREAM Software Performance	119
<i>Christophe De Cannière</i>	
DECIM ^{v2}	140
<i>Côme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Blandine Debraize, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier, Thomas Pornin, and Hervé Sibert</i>	
The Stream Cipher Edon80	152
<i>Daniło Gligoroski, Smile Markovski, and Svein Johan Knapskog</i>	

F-FCSR Stream Ciphers	170
<i>François Arnault, Thierry Berger, and Cédric Lauradoux</i>	
The Grain Family of Stream Ciphers	179
<i>Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier</i>	
The MICKEY Stream Ciphers	191
<i>Steve Babbage and Matthew Dodd</i>	
The Self-synchronizing Stream Cipher MOUSTIQUE	210
<i>Joan Daemen and Paris Kitsos</i>	
Cascade Jump Controlled Sequence Generator and Pomaranch Stream Cipher	224
<i>Cees J.A. Jansen, Tor Helleseth, and Alexander Kholosha</i>	
TRIVIUM	244
<i>Christophe De Cannière and Bart Preneel</i>	
ASIC Hardware Performance	267
<i>Tim Good and Mohammed Benaïssa</i>	
Author Index	295