Lecture Notes in Computer Science 4986

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Matthew Robshaw Olivier Billet (Eds.)

New Stream Cipher Designs

The eSTREAM Finalists

Springer

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

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 administrational 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 cryptanalyzed, 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