

Lecture Notes in Computer Science

2365

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Joan Daemen Vincent Rijmen (Eds.)

Fast Software Encryption

9th International Workshop, FSE 2002
Leuven, Belgium, February 4-6, 2002
Revised Papers



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Joan Daemen
Proton World
Zweefvliegtuigstraat 10
1130 Brussel, Belgium
E-mail: joan.daemen@protonworld.com

Vincent Rijmen
Cryptomathic
Lei 8A
3000 Leuven, Belgium
E-mail: vincent.rijmen@cryptomathic.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fast software encryption : 9th international workshop ; revised papers / FSE 2002, Leuven, Belgium, February 2002. Joan Daemen ; Vincent Rijmen (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2365)
ISBN 3-540-44009-7

CR Subject Classification (1998): E.3, F.2.1, E.4, G.4

ISSN 0302-9743

ISBN 3-540-44009-7 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, especially 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York,
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e.K.
Printed on acid-free paper SPIN: 10870318 06/3142 5 4 3 2 1 0

Preface

This Fast Software Encryption workshop was the ninth in a series of workshops started in Cambridge in December 1993. The previous workshop took place in Yokohama in April 2001. It concentrated on all aspects of fast primitives for symmetric cryptography: secret key ciphers, the design and cryptanalysis of block and stream ciphers, as well as hash functions and message authentication codes (MACs).

The ninth Fast Software Encryption workshop was held in February 2002 in Leuven, Belgium and was organized by General Chair Matt Landrock (Cryptomathic Belgium), in cooperation with the research group COSIC of K.U. Leuven. This year there were 70 submissions, of which 21 were selected for presentation and publication in this volume.

We would like to thank the following people. First of all the submitting authors and the program committee for their work. Then Markku-Juhani O. Saarinen, Orr Dunkelman, Fredrik Jönsson, Helger Lipmaa, Greg Rose, Alex Biryukov, and Christophe De Canniere, who provided reviews at the request of program committee members. Bart Preneel for letting us use COSIC's Web-review software in the review process and Wim Moreau for all his support. Finally we would like to thank Krista Geens of Cryptomathic for her help in the registration and the practical organization.

May 2002

Joan Daemen and Vincent Rijmen

Fast Software Encryption 2002

February 4–6, 2002, Leuven, Belgium

Sponsored by the
International Association for Cryptologic Research

General Chair

Matt Landrock, Cryptomathic, Belgium

Program Co-chairs

Joan Daemen, Proton World, Belgium
Vincent Rijmen, Cryptomathic, Belgium

Program Committee

Ross Anderson	Cambridge University, UK
Eli Biham	Technion, IL
Don Coppersmith	IBM, USA
Cunshen Ding	Hong Kong University of Science and Technology, HK
Thomas Johansson	Lund University, SE
Mitsuru Matsui	Mitsubishi Electric, JP
Willi Meier	Fachhochschule Aargau, CH
Kaisa Nyberg	Nokia, FI
Bart Preneel	Katholieke Universiteit Leuven, BE

Table of Contents

Block Cipher Cryptanalysis

New Results on Boomerang and Rectangle Attacks	1
<i>Eli Biham, Orr Dunkelman, and Nathan Keller (Technion – Israel Institute of Technology)</i>	
Multiplicative Differentials	17
<i>Nikita Borisov, Monica Chew, Rob Johnson, and David Wagner (University of California at Berkeley)</i>	
Differential and Linear Cryptanalysis of a Reduced-Round SC2000	34
<i>Hitoshi Yanami, Takeshi Shimoyama (Fujitsu Laboratories Ltd.), and Orr Dunkelman (Technion – Israel Institute of Technology)</i>	
Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA	49
<i>Dukjae Moon, Kyungdeok Hwang, Wonil Lee, Sangjin Lee, and Jongin Lim (Center for Information and Security Technologies, Korea University)</i>	
Improved Cryptanalysis of MISTY1	61
<i>Ulrich Kühn (Dresdner Bank AG)</i>	
Multiple Linear Cryptanalysis of a Reduced Round RC6	76
<i>Takeshi Shimoyama, Masahiko Takenaka, and Takeshi Koshihara (Fujitsu Laboratories Ltd.)</i>	

Integral Cryptanalysis

On the Security of CAMELLIA against the Square Attack	89
<i>Yongjin Yeom, Sangwoo Park, and Iljun Kim (National Security Research Institute Korea)</i>	
Saturation Attacks on Reduced-Round Skipjack	100
<i>Kyungdeok Hwang, Wonil Lee (Center for Information and Security Technologies (CIST) Korea University), Sungjae Lee (Korea Information Security Agency), Sangjin Lee, and Jongin Lim (CIST), Korea University</i>	
Integral Cryptanalysis	112
<i>Lars Knudsen (Dept. of Mathematics, DTU) and David Wagner (University of California at Berkeley)</i>	

Block Cipher Theory

Improved Upper Bounds of Differential and Linear Characteristic Probability for Camellia	128
<i>Taizo Shirai, Shoji Kanamaru, and George Abe (Sony Corporation)</i>	
The Round Functions of RIJNDAEL Generate the Alternating Group	143
<i>Ralph Wernsdorf (Rohde & Schwarz SIT GmbH)</i>	
Non-cryptographic Primitive for Pseudorandom Permutation	149
<i>Tetsu Iwata, Tomonobu Yoshino (Tokyo Institute of Technology), and Kaoru Kurosawa (Ibaraki University)</i>	

Stream Cipher Design

BeepBeep: Embedded Real-Time Encryption	164
<i>Kevin Driscoll (Honeywell Laboratories)</i>	
A New Keystream Generator MUGI.....	179
<i>Dai Watanabe, Soichi Furuya, Hirotaka Yoshida, Kazuo Takaragi (Hitachi), and Bart Preneel (K.U. Leuven, Dept. ESAT)</i>	
Scream: A Software-Efficient Stream Cipher	195
<i>Shai Halevi, Don Coppersmith, and Charanjit Jutla (IBM T.J. Watson Research Center)</i>	

Stream Cipher Cryptanalysis

Distinguishing Attacks on SOBER-t16 and t32	210
<i>Patrik Ekdahl and Thomas Johansson (Dept. of Information Technology, Lund University)</i>	
Linearity Properties of the SOBER-t32 Key Loading	225
<i>Markus Dichtl and Marcus Schafheutle (Siemens AG)</i>	
A Time-Memory Tradeoff Attack against LILI-128	231
<i>Markku-Juhani Olavi Saarinen (Helsinki University of Technology)</i>	

Odds and Ends

On the Security of Randomized CBC-MAC beyond the Birthday Paradox Limit: A New Construction.....	237
<i>Éliane Jaulmes, Antoine Joux, and Frédéric Valette (DCSSI Crypto Lab)</i>	
Cryptanalysis of the Modified Version of the Hash Function Proposed at PKC'98	252
<i>Daewan Han, Sangwoo Park, and Seongtaek Chee (National Security Research Institute Korea)</i>	

Compression and Information Leakage of Plaintext	263
<i>John Kelsey (Certicom)</i>	
Author Index	277