

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

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

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Henri Gilbert Helena Handschuh (Eds.)

Fast Software Encryption

12th International Workshop, FSE 2005
Paris, France, February 21-23, 2005
Revised Selected Papers



Springer

Volume Editors

Henri Gilbert

France Telecom, 92794 Issy les Moulineaux, France

E-mail: henri.gilbert@francetelecom.com

Helena Handschuh

Gemplus SA, Issy-les-Moulineaux, France

E-mail: Helena.Handschuh@gemplus.com

Library of Congress Control Number: 2005928340

CR Subject Classification (1998): E.3, F.2.1, E.4, G.2, G.4

ISSN 0302-9743

ISBN-10 3-540-26541-4 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-26541-2 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

springeronline.com

© International Association for Cryptologic Research 2005

Printed in Germany

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

Printed on acid-free paper SPIN: 11502760 06/3142 5 4 3 2 1 0

Preface

The Fast Software Encryption 2005 Workshop was the twelfth in a series of annual workshops on symmetric cryptography, sponsored for the fourth year by the International Association for Cryptologic Research (IACR). The workshop concentrated on all aspects of fast primitives for symmetric cryptology, including the design, cryptanalysis and implementation of block and stream ciphers as well as hash functions and message authentication codes. The first FSE workshop was held in Cambridge in 1993, followed by Leuven in 1994, Cambridge in 1996, Haifa in 1997, Paris in 1998, Rome in 1999, New York in 2000, Yokohama in 2001, Leuven in 2002, Lund in 2003, and New Delhi in 2004.

This year, a total of 96 submissions were received. After an extensive review by the Program Committee, 30 submissions were accepted. Two of these submissions were merged into a single paper, yielding a total of 29 papers accepted for presentation at the workshop. Also, we were very fortunate to have in the program an invited talk by Xuejia Lai on “Attacks and Protection of Hash Functions” and a very entertaining rump session that Bart Preneel kindly accepted to chair. These proceedings contain the revised versions of the accepted papers; the revised versions were not subsequently checked for correctness.

We are very grateful to the Program Committee members and to the external reviewers for their hard work. Each paper was refereed by at least three reviewers, and at least five reviewers in the case of papers (co-)authored by Program Committee members; eventually, an impressive total of 334 reviews was produced. Special thanks are also due to the members of the Local Organizing Committee, Côme Berbain, Olivier Billet (who designed the FSE 2005 Web pages and assembled the preproceedings), Julien Bouchier (who managed the submission and Webreview servers), Stanislas Francfort, Aline Gouget, Françoise Levy, Pierre Loidreau, and Pascal Paillier (who managed on-site registration), for their generous efforts and strong support.

Many thanks to Kevin McCurley for handling the registration server, to Patrick Arditti, Virginie Berger and Claudine Campolunghi for providing assistance with the registration process, and to the research group COSIC of the K.U.Leuven for kindly providing their Webreview software.

Last but not least, we would like to thank the conference sponsors France Telecom, Gemplus, and Nokia for their financial support, DGA and ENSTA for hosting the conference on their premises, and all submitters and workshop participants who made this year’s workshop such an enjoyable event.

FSE 2005

February 21–23, 2005, Paris, France

Sponsored by
the International Association for Cryptologic Research (IACR)

Program and General Chairs

Henri Gilbert France Telecom, France
Helena Handschuh Gemplus, France

Program Committee

Kazumaro Aoki NTT, Japan
Steve Babbage Vodafone, UK
Eli Biham Technion, Israel
Anne Canteaut INRIA, France
Don Coppersmith IBM Research, USA
Joan Daemen STMicroelectronics, Belgium
Thomas Johansson Lund University, Sweden
Antoine Joux DGA and Université de Versailles, France
Xuejia Lai Shanghai Jiaotong University, China
Stefan Lucks Universität Mannheim, Germany
Mitsuru Matsui Mitsubishi Electric, Japan
Willi Meier FH Aargau, Switzerland
Kaisa Nyberg Nokia, Finland
Bart Preneel K.U.Leuven, Belgium
Matt Robshaw Royal Holloway, University of London, UK
Palash Sarkar Indian Statistical Institute, India
Serge Vaudenay EPFL, Switzerland
Moti Yung Columbia University, USA

Local Organizing Committee

Côme Berbain, Olivier Billet, Julien Bouchier, Stanislas Francfort, Henri Gilbert, Aline Gouget, Helena Handschuh, Françoise Levy, Pierre Loidreau, Pascal Paillier

Industry Sponsors

France Telecom
Gemplus SA
Nokia

External Referees

Frederik Armknecht
Daniel Augot
Gildas Avoine
Thomas Baignères
Elad Barkan
An Braeken
Claude Carlet
Pascale Charpin
Sanjit Chatterjee
Rafi Chen
Debra L. Cook
Christophe De Cannière
Orr Dunkelman
Matthieu Finiasz
Pierre-Alain Fouque
Soichi Furuya
Louis Granboulan
Tor Helleseth
Shoichi Hirose
Tetsu Iwata
Pascal Junod
Charanjit Jutla
Grigory Kabatyanskiy
Jonathan Katz
Alexander Kholosha
Yuichi Komano
Matthias Krause
Ulrich Kühn

Simon Künzli
Shreekanth Laksmeshwar
Joseph Lano
Cédric Lauradoux
Yi Lu
Marine Minier
Håvard Molland
Jean Monnerat
Shiho Moriai
Frédéric Muller
Sean Murphy
Philippe Oechslin
Kenji Ohkuma
Katsuyuki Okeya
Elisabeth Oswald
Souradyuti Paul
Gilles Piret
Zulfikar Ramzan
Vincent Rijmen
Akashi Satoh
Takeshi Shimoyama
Taizo Shirai
François-Xavier Standaert
Dirk Stegemann
Henk van Tilborg
Hiroki Ueda
Kan Yasuda
Erik Zenner

Table of Contents

New Designs

A New MAC Construction ALRED and a Specific Instance ALPHA-MAC <i>Joan Daemen, Vincent Rijmen</i>	1
New Applications of T-Functions in Block Ciphers and Hash Functions <i>Alexander Klimov, Adi Shamir</i>	18
The Poly1305-AES Message-Authentication Code <i>Daniel J. Bernstein</i>	32

Stream Ciphers I

Narrow T-Functions <i>Magnus Daum</i>	50
A New Class of Single Cycle T-Functions <i>Jin Hong, Dong Hoon Lee, Yongjin Yeom, Daewan Han</i>	68
F-FCSR: Design of a New Class of Stream Ciphers <i>François Arnault, Thierry P. Berger</i>	83

Boolean Functions

Cryptographically Significant Boolean Functions: Construction and Analysis in Terms of Algebraic Immunity <i>Deepak Kumar Dalai, Kishan Chand Gupta, Subhamoy Maitra</i>	98
The ANF of the Composition of Addition and Multiplication mod 2^n with a Boolean Function <i>An Braeken, Igor Semaev</i>	112

Block Ciphers I

New Combined Attacks on Block Ciphers <i>Eli Biham, Orr Dunkelman, Nathan Keller</i>	126
Small Scale Variants of the AES <i>Carlos Cid, Sean Murphy, Matt J.B. Robshaw</i>	145

Stream Ciphers II

Unbiased Random Sequences from Quasigroup String Transformations
Smile Markovski, Danilo Gligoroski,
Ljupco Kocarev 163

A New Distinguisher for Clock Controlled Stream Ciphers
Håkan Englund, Thomas Johansson 181

Analysis of the Bit-Search Generator and Sequence Compression
Techniques
Aline Gouget, Hervé Sibert, Côme Berbain, Nicolas Courtois,
Blandine Debraize, Chris Mitchell 196

Some Attacks on the Bit-Search Generator
Martin Hell, Thomas Johansson 215

Hash Functions

SMASH - A Cryptographic Hash Function
Lars R. Knudsen 228

Security Analysis of a 2/3-Rate Double Length Compression Function
in the Black-Box Model
Mridul Nandi, Wonil Lee, Kouichi Sakurai,
Sangjin Lee 243

Preimage and Collision Attacks on MD2
Lars R. Knudsen and John E. Mathiassen 255

Modes of Operation

How to Enhance the Security of the 3GPP Confidentiality and Integrity
Algorithms
Tetsu Iwata, Kaoru Kurosawa 268

Two-Pass Authenticated Encryption Faster Than Generic Composition
Stefan Lucks 284

Padding Oracle Attacks on CBC-Mode Encryption with Secret and
Random IVs
Arnold K.L. Yau, Kenneth G. Paterson,
Chris J. Mitchell 299

Stream Ciphers III

Analysis of the Non-linear Part of Mugi <i>Alex Biryukov, Adi Shamir</i>	320
Two Attacks Against the HBB Stream Cipher <i>Antoine Joux, Frédéric Muller</i>	330
Two Linear Distinguishing Attacks on VMPC and RC4A and Weakness of RC4 Family of Stream Ciphers <i>Alexander Maximov</i>	342
Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4 <i>Eli Biham, Louis Granboulan, Phong Q. Nguyễn</i>	359

Block Ciphers II

Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192 <i>Seokhie Hong, Jongsung Kim, Sangjin Lee, Bart Preneel</i>	368
New Attacks Against Reduced-Round Versions of IDEA <i>Pascal Junod</i>	384

Implementations

How to Maximize Software Performance of Symmetric Primitives on Pentium III and 4 Processors <i>Mitsuru Matsui, Sayaka Fukuda</i>	398
A Side-Channel Analysis Resistant Description of the AES S-Box <i>Elisabeth Oswald, Stefan Mangard, Norbert Pramstaller, Vincent Rijmen</i>	413
DPA Attacks and S-Boxes <i>Emmanuel Prouff</i>	424
Author Index	443