Lecture Notes in Computer Science 3557

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

Editorial Board

Henri Gilbert Helena Handschuh (Eds.)

Fast Software Encryption

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

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

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 Brouchier (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.

April 2005 Henri Gilbert and Helena Handschuh

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 Brouchier, 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

Stream Ciphers II

Hash Functions

Modes of Operation

Stream Ciphers III

Block Ciphers II

Implementations