

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

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*

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Bimal Roy Willi Meier (Eds.)

# Fast Software Encryption

11th International Workshop, FSE 2004  
Delhi, India, February 5-7, 2004  
Revised Papers



Springer

## Volume Editors

Bimal Roy

Applied Statistics Unit, Indian Statistical Institute

203, B.T. Road, Calcutta 700 108, India

E-mail: bimal@isical.ac.in

Willi Meier

FH Aargau, 5210 Windisch, P.O. Box , Switzerland

E-mail: meierw@fh-aargau.ch

Library of Congress Control Number: 2004107501

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

ISSN 0302-9743

ISBN 3-540-22171-9 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, 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-Verlag. Violations are liable to prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004

Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein

Printed on acid-free paper      SPIN: 11011880      06/3142      5 4 3 2 1 0

# Preface

Fast Software Encryption is a now eleven years old workshop on symmetric cryptography, including the design and analysis of block ciphers and stream ciphers as well as hash functions and message authentication codes. The FSE workshop was first 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, and Lund in 2003.

This Fast Software Encryption Workshop, FSE 2004, was held February 5–7, 2004 in Delhi, India. The workshop was sponsored by IACR (the International Association for Cryptologic Research) and organized in cooperation with the Indian Statistical Institute, Delhi, and the Cryptology Research Society of India (CRSI).

This year a total of 75 papers were submitted to FSE 2004. After a seven week reviewing process, 28 papers were accepted for presentation at the workshop. In addition, we were fortunate to have in the program two invited talks by Adi Shamir and David Wagner.

During the workshop a rump section was held. Seven presentations were made and all the presenters were given the option of submitting their presentations for possible inclusion in the proceedings. Only one paper from this session was submitted, which was refereed and accepted. This paper appears at the end of these proceedings.

We would like to thank the following people. First Springer-Verlag for publishing the proceedings in the Lecture Notes in Computer Science series. Next the submitting authors, the committee members, the external reviewers, the general co-chairs Subhamoy Maitra and R.L. Karandikar, and the local organizing committee, for their hard work. Bart Preneel for letting us use COSIC's Webreview software in the review process and Thomas Herlea for his support. We are indebted to Lund University, especially Thomas Johansson, Bijit Roy and Sugata Gangopadhyay for hosting the Webreview site. Additionally we would like to thank Partha Mukhopadhyay, Sourav Mukhopadhyay, Malapati Raja Sekhar, and Chandan Biswas for handling all the submissions and Madhusudan Karan for putting together the pre-proceedings. We would also like to thank the sponsors: Infosys Technology Ltd., Honeywell Corporation and Via Technology.

The organizing committee consisted of Sanjay Burman (CAIR, Bangalore), Ramendra S. Baoni (Bisecure Technologies Pvt. Ltd., Delhi), Hiranmoy Ghosh (Tata Infotech Ltd. Delhi), Abdul Sakib Mondal (Infosys Technologies Ltd., Bangalore), Arup Pal (ISI, Delhi), N.R. Pillai (SAG, Delhi), P.K.Saxena (SAG, Delhi), and Amitabha Sinha (ISI, Kolkata), who served as Treasurer. Thank you to them all.

# Fast Software Encryption 2004

February 5–7, 2004, Delhi, India

Sponsored by the  
*International Association for Cryptologic Research*

in cooperation with the  
*Indian Statistical Institute, Delhi*  
and  
*Cryptology Research Society of India*

## General Co-chairs

Subhamoy Maitra, Indian Statistical Institute, Kolkata  
and  
R.L. Karandikar, Indian Statistical Institute, Delhi

## Program Co-chairs

Bimal Roy, Indian Statistical Institute, Kolkata  
and  
Willi Meier, Fachhochschule Aargau, Switzerland

## Program Committee

Eli Biham	Technion Israel
Claude Carlet	INRIA, France
Don Coppersmith	IBM, USA
Cunsheng Ding	Hong Kong University of Science and Technology
Helena Handschuh	Gemplus, France
Thomas Johansson	Lund University, Sweden
Charanjit S. Jutla	IBM Research, USA
Lars R. Knudsen	Technical University of Denmark
Kaoru Kurosawa	Ibaraki University, Japan
Kaisa Nyberg	Nokia, Finland
C. Pandu Rangan	Indian Institute of Technology, Chennai
Dingyi Pei	Chinese Academy of Sciences
Bart Preneel	K.U. Leuven, Belgium
Matt Robshaw	Royal Holloway, University of London, U.K.
Serge Vaudenay	EPFL, Switzerland
C.E. Veni Madhavan	Indian Institute of Science, Bangalore
Xian-Mo Zhang	Macquarie University, Australia

## External Reviewers

Gildas Avoine  
Thierry Berger  
Christophe Clavier  
Orr Dunkelman  
Marc Girault  
Shoichi Hirose  
Fredrik Jönsson  
Ju-Sung Kang  
Yong Li  
Marine Minier  
Enes Pasalic  
Haavard Raddum  
Xiaojian Tian  
Akihiro Yamamura

Thomas Baignères  
Qingjun Cai  
Nicolas Courtois  
Eric Filiol  
Philippe Guillot  
Tetsu Iwata  
Jakob Johnsson  
Tania Lange  
Yi Lu  
Jean Monnerat  
Souradyuti Paul  
Palash Sarkar  
Xuesong Wang  
Julien Bouchier

Elad Barkan  
Carlos Cid  
Christophe De Cannière  
Henri Gilbert  
Louis Guillou  
Thomas Jakobsen  
Pascal Junod  
Joseph Lano  
Miodrag Mihaljevic  
Sean Murphy  
Michael Quisquater  
Takeshi Shimoyama  
Guohua Xiong  
Ju-Sung Kang

# Table of Contents

New Cryptographic Primitives Based on Multiword T-Functions <i>Alexander Klimov and Adi Shamir</i> .....	1
Towards a Unifying View of Block Cipher Cryptanalysis <i>David Wagner</i> .....	16
Algebraic Attacks on Summation Generators <i>Dong Hoon Lee, Jaeheon Kim, Jin Hong, Jae Woo Han, and Dukjae Moon</i> .....	34
Algebraic Attacks on SOBER-t32 and SOBER-t16 without Stuttering <i>Joo Yeon Cho and Josef Pieprzyk</i> .....	49
Improving Fast Algebraic Attacks <i>Frederik Armknecht</i> .....	65
Resistance of S-Boxes against Algebraic Attacks <i>Jung Hee Cheon and Dong Hoon Lee</i> .....	83
Differential Attacks against the Helix Stream Cipher <i>Frédéric Muller</i> .....	94
Improved Linear Consistency Attack on Irregular Clocked Keystream Generators <i>Håvard Molland</i> .....	109
Correlation Attacks Using a New Class of Weak Feedback Polynomials <i>Håkan Englund, Martin Hell, and Thomas Johansson</i> .....	127
Minimum Distance between Bent and 1-Resilient Boolean Functions <i>Soumen Maity and Subhamoy Maitra</i> .....	143
Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions <i>Pantelimon Stănică, Subhamoy Maitra, and John A. Clark</i> .....	161
A Weakness of the Linear Part of Stream Cipher MUGI <i>Jovan Dj. Golić</i> .....	178
Vulnerability of Nonlinear Filter Generators Based on Linear Finite State Machines <i>Jin Hong, Dong Hoon Lee, Seongtaek Chee, and Palash Sarkar</i> .....	193
VMPC One-Way Function and Stream Cipher <i>Bartosz Zoltak</i> .....	210



A New Stream Cipher HC-256 <i>Hongjun Wu</i> .....	226
A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher <i>Souradyuti Paul and Bart Preneel</i> .....	245
Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS Matrices <i>Taizo Shirai and Kyoji Shibutani</i> .....	260
ICEBERG : An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware <i>Francois-Xavier Standaert, Gilles Piret, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat</i> .....	279
Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST <i>Youngdai Ko, Seokhie Hong, Wonil Lee, Sangjin Lee, and Ju-Sung Kang</i> ..	299
On the Additive Differential Probability of Exclusive-Or <i>Helger Lipmaa, Johan Wallén, and Philippe Dumas</i> .....	317
Two Power Analysis Attacks against One-Mask Methods <i>Mehdi-Laurent Akkar, Régis Bévan, and Louis Goubin</i> .....	332
Nonce-Based Symmetric Encryption <i>Phillip Rogaway</i> .....	348
Ciphers Secure against Related-Key Attacks <i>Stefan Lucks</i> .....	359
Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance <i>Phillip Rogaway and Thomas Shrimpton</i> .....	371
The EAX Mode of Operation <i>Mihir Bellare, Phillip Rogaway, and David Wagner</i> .....	389
CWC: A High-Performance Conventional Authenticated Encryption Mode <i>Tadayoshi Kohno, John Viega, and Doug Whiting</i> .....	408
New Security Proofs for the 3GPP Confidentiality and Integrity Algorithms <i>Tetsu Iwata and Tadayoshi Kohno</i> .....	427
Cryptanalysis of a Message Authentication Code due to Cary and Venkatesan <i>Simon R. Blackburn and Kenneth G. Paterson</i> .....	446

Fast Software-Based Attacks on SecurID <i>Scott Contini and Yiqun Lisa Yin</i> .....	454
A MAC Forgery Attack on SOBER-128 <i>Dai Watanabe and Soichi Furuya</i> .....	472
On Linear Approximation of Modulo Sum <i>Alexander Maximov</i> .....	483
<b>Author Index</b> .....	485