Lecture Notes in Computer Science 3017

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

Editorial Board

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

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.

February 2004 Bimal Roy and Willi Meier

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
Thomas Baignères
Elad Barkan
Thierry Berger
Qingjun Cai
Carlos Cid
Christophe Clavier
Nicolas Courtois
Christophe De Cannière
Orr Dunkelman
Eric Filiol
Henri Gilbert
Marc Girault
Philippe Guillot
Louis Guillou
Shoichi Hirose
Tetsu Iwata
Thomas Jakobsen
Fredrik Jönsson
Jakob Johnsson
Pascal Junod
Ju-Sung Kang
Tania Lange
Joseph Lano
Yong Li
Yi Lu
Miodrag Mihaljevic
Marine Minier
Jean Monnerat
Sean Murphy
Enes Pasalic
Souradyuti Paul
Michael Quisquater
Haavard Raddum
Palash Sarkar
Takeshi Shimoyama
Xiaojian Tian
Xuesong Wang
Guohua Xiong
Akihiro Yamamura
Julien Brouchier
Ju-Sung Kang

Table of Contents