Lecture Notes in Computer Science 3357

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

## Editorial Board

Helena Handschuh M. Anwar Hasan (Eds.)

# Selected Areas in Cryptography

11th International Workshop, SAC 2004
Waterloo, Canada, August 9-10, 2004
Revised Selected Papers

Springer

Volume Editors

Helena Handschuh
Gemplus, Issy-les-Moulineaux, France
E-mail: Helena.Handschuh@gemplus.com

M. Anwar Hasan
University of Waterloo, Waterloo, Ontario, Canada
E-mail: ahasan@ece.uwaterloo.ca

Library of Congress Control Number: 2004117402

CR Subject Classification (1998): E.3, D.4.6, K.6.5, F.2.1-2, C.2, H.4.3

ISSN 0302-9743
ISBN 3-540-24327-5 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11376224 06/3142 5 4 3 2 1 0

# Preface

SAC 2004 was the eleventh in a series of annual workshops on Selected Areas in Cryptography. This was the second time that the workshop was hosted by the University of Waterloo, Ontario, with previous workshops being held at Queen's University in Kingston (1994, 1996, 1998 and 1999), Carleton University in Ottawa (1995, 1997 and 2003), the Fields Institute in Toronto (2001) and Memorial University of Newfoundland in St. John's (2002). The primary intent of the workshop was to provide a relaxed atmosphere in which researchers in cryptography could present and discuss new work on selected areas of current interest. This year's themes for SAC were:

- Design and analysis of symmetric key cryptosystems.
- Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms.
- Efficient implementation of cryptographic systems in public and symmetric key cryptography.
- Cryptographic solutions for mobile (web) services.

A record of 117 papers were submitted for consideration by the program committee. After an extensive review process, 25 papers were accepted for presentation at the workshop (two of these papers were merged). Unfortunately, many good papers could not be accommodated this year. These proceedings contain the revised versions of the 24 accepted papers. The revised versions were not subsequently checked for correctness.

Also, we were very fortunate to have two invited speakers at SAC 2004.

- Eli Biham arranged for some breaking news in his talk on "New Results on SHA-0 and SHA-1." This talk was designated as the Stafford Tavares Lecture.
- Yevgeniy Dodis enlightened us with "Basing Cryptography on Biometrics and Other Noisy Data."

We are very grateful to the program committee and to the numerous external reviewers for their hard work and precious help. They collectively produced over 380 review reports in less than two months, which was quite a challenge. We have tried to list all of them in these proceedings and we sincerely hope we did not omit anyone.

We are also indebted to the University of Waterloo, Queen's University Kingston, Mitsubishi Electric Corporation, and Research in Motion Ltd. for their financial support of the workshop.

Special thanks are due to K.U.Leuven for kindly providing the Webreview software, Julien Brouchier for running both the submission server and Webreview, Janet Bullock for perfectly handling registrations, and Jaewook Chung and

the local arrangements committee from the University of Waterloo for setting up the website and organizing a very nice and entertaining workshop.

Last but not least we would like to thank all submitters and all the participants who made this year's workshop a great success.

November 2004 Helena Handschuh and M. Anwar Hasan

# 11th Annual Workshop on Selected Areas in Cryptography

August 9–10, 2004, Waterloo, Ontario, Canada

## Program and General Chairs

Helena Handschuh ..... Gemplus, France
M. Anwar Hasan ..... University of Waterloo, Canada

## Program Committee

Carlisle Adams ..... University of Ottawa, Canada
Henri Gilbert ..... France Télécom, France
Mike Just ..... Carleton University, Canada
Charanjit Jutla ..... IBM, USA
Arjen Lenstra ..... Lucent Technologies, USA
and T.U. Eindhoven, The Netherlands
Stefan Lucks ..... Universität Mannheim, Germany
Mitsuru Matsui ..... Mitsubishi Electric, Japan
Alfred Menezes ..... University of Waterloo, Canada
Shiho Moriai ..... Sony Computer Entertainment Inc., Japan
Kaisa Nyberg ..... Nokia, Finland
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Matt Robshaw ..... Royal Holloway University of London, UK
Douglas R. Stinson ..... University of Waterloo, Canada
Serge Vaudenay ..... EPFL, Switzerland
Michael Wiener ..... Cryptographic Clarity, Canada

## Local Arrangements Committee

Janet Bullock, Jaewook Chung, Agustin Dominguez, M. Anwar Hasan, Arash Reyhani-Masoleh, and Siavash B. Sarmadi

## Sponsors

University of Waterloo
Mitsubishi Electric Corporation
Research in Motion Ltd.
Queen's University Kingston

## External Referees

Frederik Armknecht
Gildas Avoine
Steve Babbage
Thomas Baignères
Lejla Batina
Come Berbain
Florent Bersani
Eli Biham
Olivier Billet
Antoon Bosselaers
Eric Brier
Jaewook Chung
Carlos Cid
Jean-Sébastien Coron
Nicolas Courtois
Paolo D'Arco
Christophe De Cannière
Nevine Ebeid
Soichi Furuya
Guang Gong
Louis Goubin
Shai Halevi
Darrel Hankerson
Jason Hinek
Daisuke Inoue
Tetsu Iwata
Shaoquan Jiang
Antoine Joux
Pascal Junod
Masayuki Kanda
John Kelsey
Kazukuni Kobara
Matthias Krause
Ulrich Kühn
Joseph Lano
Yi Lu
Jonathan Lutz
Kazuhiko Minematsu
Serge Mister
Jean Monnerat
Sumio Morioka
James Muir
Sean Murphy
Junko Nakajima
Kazuomi Oishi
Sıddıka Berna Örs
Matthew Parker
Kenny Paterson
Josyula R. Rao
Arash Reyhani-Masoleh
Pankaj Rohatgi
Taiichi Saito
Fumihiko Sano
Akashi Satoh
Werner Schindler
Jasper Scholten
Kyoji Shibutani
Takeshi Shimoyama
Taizo Shirai
Dirk Stegemann
Daisuke Suzuki
Jacques Traoré
Dai Watanabe
Brecht Wyseur
Yongjin Yeom
Erik Zenner
Robert Zuccherato

# Table of Contents

## Secret Key Cryptography I



## Cryptanalysis



## Cryptographic Protocols

## Secret Key Cryptography II