

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

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

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

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

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

Table of Contents

Stream Cipher Cryptanalysis

An Improved Correlation Attack on A5/1 <i>Alexander Maximov, Thomas Johansson, Steve Babbage</i>	1
Extending the Resynchronization Attack <i>Frederik Armknecht, Joseph Lano, Bart Preneel</i>	19
A New Simple Technique to Attack Filter Generators and Related Ciphers <i>Håkan Englund, Thomas Johansson</i>	39

Side-Channel Analysis

On XTR and Side-Channel Analysis <i>Daniel Page, Martijn Stam</i>	54
Provably Secure Masking of AES <i>Johannes Blömer, Jorge Guajardo, Volker Krummel</i>	69

Block Cipher Design

Perfect Diffusion Primitives for Block Ciphers – Building Efficient MDS Matrices <i>Pascal Junod, Serge Vaudenay</i>	84
Security of the MISTY Structure in the Luby-Rackoff Model: Improved Results <i>Gilles Piret, Jean-Jacques Quisquater</i>	100
FOX: A New Family of Block Ciphers <i>Pascal Junod, Serge Vaudenay</i>	114

Efficient Implementations

A Note on the Signed Sliding Window Integer Recoding and a Left-to-Right Analogue <i>Roberto Maria Avanzi</i>	130
---	-----

Fast Irreducibility Testing for XTR Using a Gaussian Normal Basis of Low Complexity
Soonhak Kwon, Chang Hoon Kim, Chun Pyo Hong 144

Modular Number Systems: Beyond the Mersenne Family
Jean-Claude Bajard, Laurent Imbert, Thomas Plantard 159

Efficient Doubling on Genus Two Curves over Binary Fields
Tanja Lange, Marc Stevens 170

Secret Key Cryptography I

About the Security of Ciphers (Semantic Security and Pseudo-Random Permutations)
Duong Hieu Phan, David Pointcheval 182

A Subliminal Channel in Secret Block Ciphers
Adam Young, Moti Yung 198

Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes
Pierre-Alain Fouque, Antoine Joux, Guillaume Poupard 212

Cryptanalysis

Cryptanalysis of a White Box AES Implementation
Olivier Billet, Henri Gilbert, Charaf Ech-Chatbi 227

Predicting Subset Sum Pseudorandom Generators
Joachim von zur Gathen, Igor E. Shparlinski 241

Collision Attack and Pseudorandomness of Reduced-Round Camellia
Wu Wenling, Feng Dengguo, Chen Hua 252

Cryptographic Protocols

Password Based Key Exchange with Mutual Authentication
Shaoquan Jiang, Guang Gong 267

Product Construction of Key Distribution Schemes for Sensor Networks
Reizhong Wei, Jiang Wu 280

Deterministic Key Predistribution Schemes for Distributed Sensor Networks

Jooyoung Lee, Douglas R. Stinson 294

On Proactive Secret Sharing Schemes

Ventzislav Nikov, Svetla Nikova 308

Secret Key Cryptography II

Efficient Constructions of Variable-Input-Length Block Ciphers

Sarvar Patel, Zulfikar Ramzan, Ganapathy S. Sundaram 326

A Sufficient Condition for Optimal Domain Extension of UOWHFs

Mridul Nandi 341

Author Index 355