Lecture Notes in Computer Science 2012
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Preface

SAC 2000 was the seventh in a series of annual workshops on Selected Areas in Cryptography. Previous workshops were held at Queen's University in Kingston (1994, 1996, 1998, and 1999) and at Carleton University in Ottawa (1995 and 1997). The intent of the workshops is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest.

The themes for the SAC 2000 workshop were:

- design and analysis of symmetric key cryptosystems,
- primitives for private key cryptography, including block and stream ciphers, hash functions, and MACs,
- efficient implementations of cryptographic systems in public and private key cryptography,
- cryptographic solutions for web/internet security.

A total of 41 papers were submitted to SAC 2000, one of which was subsequently withdrawn. After a review process that had all papers reviewed by at least 3 referees, 24 papers were accepted for presentation at the workshop. As well, we were fortunate to have the following two invited speakers at SAC 2000:

- M. Bellare, UCSD (U.S.A.)
  "The Provable-Security Approach to Authenticated Session-Key Exchange"
- D. Boneh, Stanford U. (U.S.A.)
  "Message Authentication in a Multicast Environment"

The program committee for SAC 2000 consisted of the following members: L. Chen, H. Heys, L. Knudsen, S. Moriai, L. O'Connor, D. Stinson, S. Tavares, S. Vaudenay, A. Youssef, and R. Zuccherato. Many thanks are due to the program committee for their hard work. Also, Amr Youssef provided great assistance in making the reviewing process run smoothly.

We are appreciative of the financial support provided by Certicom Corporation, CITO, Entrust Technologies, MITACS, and the University of Waterloo. Special thanks are due to Frances Hannigan, who was responsible for the local arrangements, and for making sure that everything ran smoothly during the workshop. Fran also assisted in preparing the workshop proceedings. Many people helped in the reviewing process by acting as sub-referees, and we appreciate all their help. Finally, we thank all the workshop participants for making SAC 2000 a success.

March 2001

Doug Stinson
Stafford Tavares

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Douglas R. Stinson Stafford Tavares (Eds.)

Selected Areas in Cryptography

7th Annual International Workshop, SAC 2000
Waterloo, Ontario, Canada, August 14-15, 2000
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Douglas R. Stinson
University of Waterloo
Department of Combinatorics and Optimization
Waterloo, Ontario, N2L 3G1, Canada
E-mail: dstinson@uwaterloo.ca

Stafford Tavares
Queen's University
Department of Electrical and Computer Engineering
Kingston, Ontario, K7L 3N6
E-mail: tavares@cc.queensu.ca

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Selected areas in cryptography : 7th annual international workshop ; proceedings / SAC 2000, Waterloo, Ontario, Canada, August 14 - 15, 2000. Douglas R. Stinson ; Stafford Tavares (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2012)
ISBN 3-540-42069-X

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

ISSN 0302-9743
ISBN 3-540-42069-X Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik Heidelberg
Printed on acid-free paper SPIN 10782303 06/3142 5 4 3 2 1 0

Organization

Program Committee

D. Stinson (co-chair)	University of Waterloo
S. Tavares (co-chair)	Queen's University at Kingston
L. Chen	Motorola (USA)
H. Heys	Memorial University of Newfoundland
L. Knudsen	University of Bergen
S. Moriai	NTT Labs. (Japan)
L. O'Connor	European Security COE (Switzerland)
S. Vaudenay	EPFL (Switzerland)
A. Youssef	University of Waterloo
R. Zuccherato	Entrust Technologies, Ottawa

Local Organizing Committee

Doug Stinson	Univesity of Waterloo
Stafford Tavares	Queen's University at Kingston
Frances Hannigan	University of Waterloo

Sponsoring Institutions

Certicom Corporation
CITO
Entrust Technologies
MITACS
University of Waterloo

Table of Contents

Cryptanalysis I

Block Ciphers – New Designs

Elliptic Curves and Efficient Implementations

Security Protocols and Applications

Block Ciphers and Hash Functions

Boolean Functions and Stream Ciphers

Public Key Systems

Cryptanalysis II