Lecture Notes in Computer Science 1556
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Stafford Tavares Henk Meijer (Eds.)

Selected Areas in Cryptography

5th Annual International Workshop, SAC'98
Kingston, Ontario, Canada, August 17-18, 1998
Proceedings

Springer

Series Editors

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

Volume Editors

Stafford Tavares
Henk Meijer
Department of Electrical and Computer Engineering
Queen's University
Kingston, Ontario K7L 3N6, Canada
E-mail: tavares@ee.queensu.ca
henk@qucis.queensu.ca

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Selected areas in cryptography : 5th annual international workshop ; proceedings / SAC '98, Kingston, Ontario, Canada, August 17 - 18, 1998. Stafford Tavares ; Henk Meijer (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1556)
ISBN 3-540-65894-7

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-65894-7 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN: 10693237 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

SAC '98 is the fifth in a series of annual workshops on Selected Areas in Cryptography. SAC '94 and SAC '96 were held at Queen's University in Kingston and SAC '95 and SAC '97 were held at Carleton University in Ottawa. The purpose of the workshop is to bring together researchers in cryptography to present new work on areas of current interest. It is our hope that focusing on selected topics will present a good opportunity for in-depth discussion in a relaxed atmosphere. The themes for the SAC '98 workshop were:

- Design and Analysis of Symmetric Key Cryptosystems
- Efficient Implementations of Cryptographic Systems
- Cryptographic Solutions for Internet Security
- Secure Wireless/Mobile Networks

Of the 39 papers submitted to SAC '98, 26 were accepted and two related papers were merged into one. There were also two invited presentations, one by Alfred Menezes entitled "Key Agreement Protocols" and the other by Eli Biham entitled "Initial Observations on SkipJack: Cryptanalysis of SkipJack-3XOR". There were 65 participants at the workshop.

The Program Committee members for SAC '98 were Carlisle Adams, Tom Cusick, Howard Heys, Henk Meijer, Doug Stinson, Stafford Tavares, Serge Vaudenay, and Michael Wiener. We also thank the following persons who acted as reviewers for SAC '98: Zhi-Guo Chen, Mike Just, Liam Keliher, Alfred Menezes, Serge Mister, Phong Nguyen, David Pointcheval, Thomas Pornin, Guillaume Poupard, Yiannis Tsioumi, Amr Youssef, and Robert Zuccherato.

This year, in addition to the Workshop Record distributed at the workshop, the papers presented at SAC '98 are published by Springer-Verlag in the Lecture Notes in Computer Science Series. Copies of the Springer Proceedings are being sent to all registrants.

The organizers of SAC '98 are pleased to thank Entrust Technologies for their financial support and Sheila Hutchison of the Department of Electrical and Computer Engineering at Queen's University for administrative and secretarial help. Yifeng Shao put together the Workshop Record and provided invaluable assistance in the preparation of these Proceedings. We also thank Laurie Ricker who looked after registration.

November 1998

Stafford Tavares and Henk Meijer
SAC '98 Co-Chairs

Organization

Program Committee

Carlisle Adams	Entrust Technologies
Tom Cusick	SUNY Buffalo
Howard Heys	Memorial University of Newfoundland
Henk Meijer	Queens University
Doug Stinson	University of Waterloo
Stafford Tavares	Queens University
Serge Vaudenay	Ecole Normale Superieure/CNRS
Mike Wiener	Entrust Technologies

Local Organizing Committee

Stafford Tavares (Co-Chair)	Queens University
Henk Meijer (Co-Chair)	Queens University

Table of Contents

Design of Secret Key Cryptosystems

Randomness and Computational Issues

Analysis of Secret Key Cryptosystems

Cryptographic Systems

Public Key Cryptosystems

Design and Implementation of Secret Key Cryptosystems

Attacks on Secret Key Cryptosystems

Invited Talks