Lecture Notes in Computer Science 2595

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Kaisa Nyberg Howard Heys (Eds.)

Selected Areas in Cryptography

9th Annual International Workshop, SAC 2002
St. John's, Newfoundland, Canada, August 15-16, 2002
Revised Papers

Springer

Volume Editors

Kaisa Nyberg
Nokia Research Center
P.O. Box 407, 00045 Nokia Group, Finland
E-mail: kaisa.nyberg@nokia.com

Howard Heys
Memorial University of Newfoundland
Faculty of Engineering and Applied Science
St. John's, NF, A1B 3X5 Canada
E-mail: howard@engr.mun.ca

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

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 3-540-00622-2 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 Boller Mediendesign
Printed on acid-free paper SPIN: 10872522 06/3142 5 4 3 2 1 0

Preface

SAC 2002 was the Ninth Annual Workshop on Selected Areas in Cryptography. Previous workshops have been held at Queen's University in Kingston (1994, 1996, 1998, and 1999), Carleton University in Ottawa (1995 and 1997), University of Waterloo (2000), and the Fields Institute in Toronto (2001). The intent of the workshop is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The traditional themes for SAC workshops are:

- Design and analysis of symmetric key cryptosystems.
- Primitives for private-key cryptography, including block and stream ciphers, hash functions, and MACs.
- Efficient implementation of cryptographic systems in public- and private-key cryptography.

The special theme for SAC 2002 was:

- Cryptographic solutions for mobile and wireless network security.

The local historic connections can be described in three words: communications, transatlantic, and wireless. After John Cabot discovered Newfoundland at the end of the 15th century, sea communication was established between that eastern outpost of the Western Hemisphere and Europe. Also in Newfoundland is Hearts Content where the first successful transatlantic cable was landed in 1866. Most remarkably, on December 12, 1901, Guglielmo Marconi reported from Signal Hill near St. John's that he successfully received the first transatlantic wireless signals, three dots, the Morse coding of letter "S," sent from Cornwall, UK.

Communication, transatlantic, and wireless were also to become the keywords of the SAC 2002 workshop held at Memorial University of Newfoundland, St. John's. There were two invited talks given by two leading cryptographers from different sides of the Atlantic Ocean presenting their views on the security of mobile and wireless communications. The invited talks were: "Security Algorithms for Mobile Telephony" by Steve Babbage from Vodafone, UK, and "Cellphone Security" by David Wagner from University of California, Berkeley.

A total of 90 papers were submitted for consideration to the program committee and after an extensive review process, 25 were accepted for presentation. We would like to thank the authors of all submitted papers, including both those that were accepted and those which, unfortunately, could not be accommodated.

We appreciate the hard work of the SAC 2002 Program Committee. We are also very grateful to the many others that participated in the review process: Jee Hea An, Kazumaro Aoki, N. Asokan, Anne Canteaut, Paolo D'Arco, Jean-François Dhem, Yael Gertner, Shai Halevi, Martin Hirt, Tetsuya Ichikawa,

Yuval Ishai, Stanislaw Jarecki, Shaoquan Jiang, Thomas Johansson, Don Johnson, Pascal Junod, Mike Just, Charanjit Jutla, Jonathan Katz, Khoongming Kho, Hugo Krawczyk, Frederic Legare, Moses Liskov, Barbara Masucci, Luke McAven, David M'Raïhi, Valtteri Niemi, Christian Paquin, Béatrice Peirani, Benny Pinkas, Omer Reingold, Ari Renvall, Phil Rogaway, Markku-Juhani Saarinen, Hong-Yeop Song, Anton Stiglic, Dong To, Eric Verheul, Johan Wallén, Rebecca Wright, and Huapeng Wu.

The local arrangements for the conference was managed by a committee consisting of Howard Heys, Paul Gillard, David Pike, Nabil Shalaby, and Lu Xiao. In particular, we would like to thank Yvonne Raymond for her help with local arrangements and registration.

Lastly, we are very grateful for the financial support that the workshop has received from Entrust Technologies, Queen's University, and the Faculty of Engineering and Applied Science of Memorial University of Newfoundland.

On behalf of all those involved in organizing the workshop, we thank all the workshop participants for making SAC 2002 a success!

December 2002 Kaisa Nyberg and Howard Heys

Organization

Program Committee

Stefan Brands	Credentica Inc., Canada
Henri Gilbert	France Telecom, France
Guang Gong	University of Waterloo, Canada
Helena Handschuh	Gemplus, France
Howard Heys (Co-chair)	Memorial University of Newfoundland, Canada
Helger Lipmaa	Helsinki University of Technology, Finland
Tal Malkin	AT&T Research, USA
Mitsuru Matsui	Mitsubishi Electric, Japan
Kaisa Nyberg (Co-chair)	Nokia Research Center, Finland
Reihaneh Safavi-Naini	University of Wollongong, Australia
Douglas Stinson	University of Waterloo, Canada
Stafford Tavares	Queen's University, Canada
Serge Vaudenay	École Polytechnique Fédérale de Lausanne, Switzerland
Michael Wiener	Ottawa, Canada
Robert Zuccherato	Entrust, Inc., Canada

Local Arrangements Committee

Howard Heys, Paul Gillard, David Pike, Yvonne Raymond, Nabil Shalaby, Lu Xiao

Sponsoring Institutions

Entrust, Inc.
Memorial University of Newfoundland
Queen's University

Table of Contents

Boolean Functions and Stream Ciphers

Block Cipher Security

Signatures and Secret Sharing

MAC and Hash Constructions

RSA and XTR Enhancements