Carlisle Adams Ali Miri Michael Wiener (Eds.)

Selected Areas in Cryptography

14th International Workshop, SAC 2007
Ottawa, Canada, August 16-17, 2007
Revised Selected Papers

Springer

Volume Editors

Carlisle Adams
University of Ottawa, School of Information Technology and Engineering (SITE)
SITE Building, 800 King Edward Avenue, Ottawa, Ontario K1N 6N5, Canada
E-mail: cadams@site.uottawa.ca

Ali Miri
University of Ottawa, School of Information Technology and Engineering (SITE)
and Department of Mathematics and Statistics
Colonel By Hall (CBY), 161 Louis Pasture Street, Ottawa, Ontario K1N 6N5, Canada
E-mail: samiri@site.uottawa.ca

Michael Wiener
Cryptographic Clarity
20 Hennepin Street, Nepean, Ontario K2J 3Z4, Canada
E-mail: michael.james.wiener@gmail.com

Library of Congress Control Number: 2007941250

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77359-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77359-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12206629 06/3180 5 4 3 2 1 0

Preface

SAC 2007 was the 14th in a series of annual workshops on Selected Areas in Cryptography. This is the first time this workshop was held at the University of Ottawa. Previous workshops were held at Queen's University in Kingston (1994, 1996, 1998, 1999, and 2005), Carleton University in Ottawa (1995, 1997, and 2003), University of Waterloo (2000 and 2004), Fields Institute in Toronto (2001), Memorial University of Newfoundland in St. Johns (2002), and Concordia University in Montreal (2006). The intent of the workshop is to provide a stimulating atmosphere where researchers in cryptology can present and discuss new work on selected areas of current interest. The themes for SAC 2007 were:

- Design and analysis of symmetric key cryptosystems
- Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms
- Efficient implementations of symmetric and public key algorithms
- Innovative cryptographic defenses against malicious software

A total of 73 papers were submitted to SAC 2007. Of these, one was withdrawn by the authors, and 25 were accepted by the Program Committee for presentation at the workshop. In addition to these presentations, we were fortunate to have two invited speakers:

- Dan Bernstein: "Edwards Coordinates for Elliptic Curves"
- Moti Yung: "Cryptography and Virology Inter-Relationships." This talk was designated the Stafford Tavares Lecture.

We are grateful to the Program Committee and the many external reviewers for their hard work and expertise in selecting the program. They completed all reviews in time for discussion and final decisions despite events conspiring to compress the review schedule. We apologize if anyone was missed in the list of external reviewers.

We would like to thank the Ontario Research Network for Electronic Commerce (ORNEC) for financial support of the workshop. We would also like to thank Gail Deduk for administrative support and Aleks Essex and Terasan Niyomsataya for technical support.

Finally, we thank all those who submitted papers and the conference participants who made this year's workshop a great success.

October 2007

Carlisle Adams
Ali Miri
Michael Wiener

14th Annual Workshop on Selected Areas in Cryptography

August 16–17, 2007, Ottawa, Ontario, Canada

in cooperation with the
International Association for Cryptologic Research (IACR)

Conference Co-chairs

Carlisle Adams	University of Ottawa, Canada
Ali Miri	University of Ottawa, Canada
Michael Wiener	Cryptographic Clarity, Canada

Program Committee

Roberto Avanzi	Ruhr University Bochum, Germany
Orr Dunkelman	Katholieke Universiteit Leuven, Belgium
Ian Goldberg	University of Waterloo, Canada
Helena Handschuh	Spansion, France
M. Anwar Hasan	University of Waterloo, Canada
Antoine Joux	DGA, Université de Versailles St-Quentin-en-Yvelines, France
Pascal Junod	Nagravision, Switzerland
Tanja Lange	Technische Universiteit, Eindhoven, Netherlands
Arjen Lenstra	EPFL, Switzerland
Christof Paar	Ruhr University Bochum, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Vincent Rijmen	Graz University of Technology, Austria
Matt Robshaw	France Telecom, France
Greg Rose	QUALCOMM, USA
Doug Stinson	University of Waterloo, Canada
Serge Vaudenay	EPFL, Switzerland
Robert Zuccherato	Entrust Inc., Canada

External Reviewers

Abdulaziz Alkhoraidly	Elena Andreeva	Thomas Baignères
Siavash Bayat-Sarmadi	Anja Becker	Côme Berbain
Daniel J. Bernstein	Eli Biham	Olivier Billet
Toni Bluher	Andrey Bogdanov	Reinier Broker

Christophe De Cannière
Scott Contini
Thomas Eisenbarth
Matthieu Finiasz
Jovan Golić
Arash Hariri
Laurent Imbert
David Jacobson
Alexandre Karlov
Cédric Lauradoux
Reynald Lercier
Marine Minier
Dag Arne Osvik
Souradyuti Paul
Emmanuel Prouff
Kai Schramm
Marc Stevens
Martin Vuagnoux
Huapeng Wu

Yaniv Carmeli
Christophe Doche
Lars Elmegaard-Fessel
Steven Galbraith
Johann Groβschädl
Phil Hawkes
Sebastiaan Indesteege
Shaoquan Jiang
Shahram Khazaei
Gregor Leander
Cameron McDonald
Bodo Möller
Elisabeth Oswald
Raphael Phan
Christian Rechberger
Yaniv Shaked
Nicolas Theriault
Johannes Wolkerstorfer
Brecht Wyseur

Jaewook Chung
Nevine Ebeid
Andreas Enge
Henri Gilbert
Tim Guneysu
Rafi Hen
Takanori Isobe
Marcelo Kaihara
Mario Lamberger
Kerstin Lemke
Florian Mendel
Jean Monnerat
Sylvain Pasini
Norbert Pramstaller
Arash Reyhani-Masoleh
Martijn Stam
Frederik Vercauteren
Hongjun Wu
Lu Xiao

Table of Contents