

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

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

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

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

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	Yaniv Carmeli	Jaewook Chung
Scott Contini	Christophe Doche	Nevine Ebeid
Thomas Eisenbarth	Lars Elmegaard-Fessel	Andreas Enge
Matthieu Finiasz	Steven Galbraith	Henri Gilbert
Jovan Golić	Johann Großschädl	Tim Guneysu
Arash Hariri	Phil Hawkes	Rafi Hen
Laurent Imbert	Sebastiaan Indestege	Takanori Isobe
David Jacobson	Shaoquan Jiang	Marcelo Kaihara
Alexandre Karlov	Shahram Khazaei	Mario Lamberger
Cédric Lauradoux	Gregor Leander	Kerstin Lemke
Reynald Lercier	Cameron McDonald	Florian Mendel
Marine Minier	Bodo Möller	Jean Monnerat
Dag Arne Osvik	Elisabeth Oswald	Sylvain Pasini
Souradyuti Paul	Raphael Phan	Norbert Pramstaller
Emmanuel Prouff	Christian Rechberger	Arash Reyhani-Masoleh
Kai Schramm	Yaniv Shaked	Martijn Stam
Marc Stevens	Nicolas Theriault	Frederik Vercauteren
Martin Vuagnoux	Johannes Wolkerstorfer	Hongjun Wu
Huapeng Wu	Brecht Wyseur	Lu Xiao

Table of Contents

Reduced Complexity Attacks on the Alternating Step Generator	1
<i>Shahram Khazaei, Simon Fischer, and Willi Meier</i>	
Extended BDD-Based Cryptanalysis of Keystream Generators	17
<i>Dirk Stegemann</i>	
Two Trivial Attacks on TRIVIUM	36
<i>Alexander Maximov and Alex Biryukov</i>	
Collisions for 70-Step SHA-1: On the Full Cost of Collision Search	56
<i>Christophe De Cannière, Florian Mendel, and Christian Rechberger</i>	
Cryptanalysis of the CRUSH Hash Function	74
<i>Matt Henricksen and Lars R. Knudsen</i>	
Improved Side-Channel Collision Attacks on AES	84
<i>Andrey Bogdanov</i>	
Analysis of Countermeasures Against Access Driven Cache Attacks on AES	96
<i>Johannes Blömer and Volker Krummel</i>	
Power Analysis for Secret Recovering and Reverse Engineering of Public Key Algorithms	110
<i>Frederic Amiel, Benoit Feix, and Karine Villegas</i>	
Koblitz Curves and Integer Equivalents of Frobenius Expansions	126
<i>Billy Bob Brumley and Kimmo Järvinen</i>	
Another Look at Square Roots (and Other Less Common Operations) in Fields of Even Characteristic	138
<i>Roberto Maria Avanzi</i>	
Efficient Explicit Formulae for Genus 2 Hyperelliptic Curves over Prime Fields and Their Implementations	155
<i>Xinxin Fan and Guang Gong</i>	
Explicit Formulas for Efficient Multiplication in \mathbb{F}_{3^m}	173
<i>Elisa Gorta, Christoph Puttmann, and Jamshid Shokrollahi</i>	
Linear Cryptanalysis of Non Binary Ciphers	184
<i>Thomas Baignères, Jacques Stern, and Serge Vaudenay</i>	
The Delicate Issues of Addition with Respect to XOR Differences	212
<i>Gaoli Wang, Nathan Keller, and Orr Dunkelman</i>	

MRHS Equation Systems	232
<i>Håvard Raddum</i>	
A Fast Stream Cipher with Huge State Space and Quasigroup Filter for Software	246
<i>Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita</i>	
Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings	264
<i>Brecht Wyseur, Wil Michiels, Paul Gorissen, and Bart Preneel</i>	
Cryptanalysis of White Box DES Implementations	278
<i>Louis Goubin, Jean-Michel Masereel, and Michaël Quisquater</i>	
Attacks on the ESA-PSS-04-151 MAC Scheme	296
<i>Georg Illies and Marian Margraf</i>	
The Security of the Extended Codebook (XCB) Mode of Operation	311
<i>David A. McGrew and Scott R. Fluhrer</i>	
A Generic Method to Design Modes of Operation Beyond the Birthday Bound	328
<i>David Lefranc, Philippe Painchault, Valérie Rouat, and Emmanuel Mayer</i>	
Passive-Only Key Recovery Attacks on RC4	344
<i>Serge Vaudenay and Martin Vuagnoux</i>	
Permutation After RC4 Key Scheduling Reveals the Secret Key	360
<i>Goutam Paul and Subhamoy Maitra</i>	
Revisiting Correlation-Immunity in Filter Generators	378
<i>Aline Gouget and Hervé Sibert</i>	
Distinguishing Attack Against TPypy	396
<i>Yukiyasu Tsunoo, Teruo Saito, Takeshi Kawabata, and Hiroki Nakashima</i>	
Author Index	409