

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Roberto Avanzi Liam Keliher
Francesco Sica (Eds.)

Selected Areas in Cryptography

15th International Workshop, SAC 2008
Sackville, New Brunswick, Canada, August 14-15
Revised Selected Papers

Volume Editors

Roberto Avanzi

Faculty of Mathematics, Ruhr University Bochum, Germany

E-mail: Roberto.Avanzi@ruhr-uni-bochum.de

Liam Keliher

Francesco Sica

Department of Mathematics and Computer Science, Mount Allison University

Sackville, New Brunswick, Canada

E-mail: {lkeliher, fsica}@mta.ca

Library of Congress Control Number: 2009933273

CR Subject Classification (1998): E.3, D.4.6, K.6.5, G.1.8, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-04158-2 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-04158-7 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.com

© Springer-Verlag Berlin Heidelberg 2009

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12738137 06/3180 5 4 3 2 1 0

Preface

The book in front of you contains the proceedings of SAC 2008, the 15th annual Workshop on Selected Areas in Cryptography. SAC 2008 took place during August 14–15 at Mount Allison University, Sackville, New Brunswick, Canada. This was the first time that SAC was hosted in New Brunswick, and the second time in an Atlantic Canadian province. Previous SAC workshops were held at Queen's University in Kingston (1994, 1996, 1998, 1999, and 2005), at Carleton University in Ottawa (1995, 1997, 2003), at the University of Waterloo (2000, 2004), at the Fields Institute in Toronto (2001), at Memorial University of Newfoundland at St. John's (2002), at Concordia University in Montreal (2006) and at the University of Ottawa (2007).

The intent of the workshop series is to provide a relaxed atmosphere in which researchers in cryptography can present and discuss new work on selected areas of current interest. The SAC workshop series has firmly established itself as an international forum for intellectual exchange in cryptological research.

The responsibility for choosing the venue of each SAC workshop and appointing the Co-chairs lies with the SAC Organizing Board. The Co-chairs then choose the Program Committee in consultation with the Board. Hence, we would like to express our gratitude to the SAC Organizing Board for giving us the mandate to organize SAC 2008, and for their invaluable feedback while assembling the Program Committee.

Starting with 2008, SAC is organized in cooperation with the International Association for Cryptologic Research (IACR). SAC 2008 witnessed two further significant events in the history of SAC. The first one was a revision of the wording of the fixed themes of the workshop. This revision takes into account trends that emerge from the papers presented at the last SAC workshops, while remaining true to the original spirit of the series. The three fixed themes are:

- *Design and analysis of symmetric key primitives and cryptosystems*
- *Efficient implementations of symmetric and public key algorithms*
- *Mathematical and algorithmic aspects of applied cryptology*

Each SAC workshop has a fourth theme which is changed every year. For SAC 2008 this was:

- *Elliptic and hyperelliptic curve cryptography, including theory and applications of pairings*

The second event was a significant increase in the number of submissions. A total of 99 technical papers were submitted to the conference from an international authorship. Of these, 27 were accepted for presentation at the workshop, a slight increase with respect to previous years, while the rate of accepted papers has been reduced. In addition to these 27 papers, two speakers were invited to give presentations at the conference.

- Jacques Patarin gave the Stafford Tavares Lecture on *The “coefficients H ” Technique*.
- Joseph Silverman gave a lecture dealing with our fourth theme, on the subject of *Lifting and the Elliptic Curve Discrete Logarithm Problem*.

The Program Committee (PC) for SAC 2008 was also the largest to date, comprising 21 members in addition to the Co-chairs. The reviewing process was a challenging task. Every paper was refereed by at least three reviewers, with papers (partially) co-authored by members of the Program Committee refereed by at least five reviewers. A total of about 310 reviews were written and uploaded by the PC members, who were helped by 107 subreviewers. The reviews were then followed by thorough discussions on the papers, which contributed in a decisive way to the quality of the final selection. About 300 additional discussion comments were written by the PC members and the Co-chairs, with up to 30 discussion comments per PC member, with some papers receiving up to 20 discussion comments. The reviews were rewritten, taking these discussions into account, before being sent to the authors. In most cases, extensive comments were sent, with one set of comments totalling 3,444 words on 477 lines – the average being about 200 lines of text per submission. Despite the huge amount of work, the atmosphere in the PC was always serene and friendly, even with some lighter moments. For us it was a honor to work with this PC.

We would like to thank the authors of all the submitted papers, both those whose work is included in these proceedings, and those whose work could not be accommodated.

The submission and review process was done using a Web-based software system developed by Shai Halevi. Changes to the system were made to accommodate our needs, and Shai replied to all our questions very quickly. We thank Shai for making his package available and for his help.

All the contributions are given in this volume in the same order as they appeared in the final program. These include revised versions of all 27 accepted submissions and the two papers related to the invited talks.

We had 71 registered participants from the following countries: Austria, Belgium, Canada, Chile, China, France, Germany, Korea, Luxembourg, Japan, The Netherlands, Singapore, Spain, Switzerland, Turkey, UK, and USA.

We also wish to express our gratitude to Mount Allison University and IEEE New Brunswick Section for financial support.

Finally we would like to thank Cindy Allan, Judith Van Rooyen, Stuart MacDonald, and Amy Adsett for helping with the organization, and all the participants of SAC 2008.

April 2009

Roberto Avanzi
Liam Keliher
Francesco Sica

Organization

SAC 2008 was organized by the SAC Organizing Board and by AceCrypt (Atlantic Centre of Excellence for Cryptographic Research), Sackville, New Brunswick, Canada in cooperation with the International Association for Cryptologic Research (IACR).

SAC Organizing Board

Carlisle Adams (Chair)	University of Ottawa, Canada
Roberto Avanzi	HGI – Ruhr Universität Bochum, Germany
Orr Dunkelman	École Normale Supérieure, France
Phil Eisen	Cloakware Corporation, Canada
Helena Handschuh	Spansion, France
Doug Stinson	University of Waterloo, Canada
Mike Wiener	Cryptographic Clarity, Canada
Adam Young	MITRE Corp, USA
Francesco Sica	AceCrypt – Mount Allison University, Canada

Program Committee

Roberto Avanzi (Co-chair)	HGI – Ruhr Universität Bochum, Germany
Paulo Barreto	Universidade de São Paulo, Brazil
Claude Carlet	Université Paris 8, France
Christophe Doche	Macquarie University, Australia
Orr Dunkelman	École Normale Supérieure, France
Joachim von zur Gathen	BIT Bonn, Germany
Elisa Gorla	Universität Zürich, Switzerland
Laurent Imbert	CNRS, PIMS–Europe – University of Calgary, Canada
Marc Joye	Thomson, France
Liam Keliher (Co-chair)	AceCrypt – Mount Allison University, Canada
Kristin Lauter	Microsoft, USA
Gregor Leander	Danmarks Tekniske Universitet, Denmark
Arjen Lenstra	EPFL Lausanne, Switzerland
Stefan Lucks	Bauhaus Universität Weimar, Germany
Tatsuaki Okamoto	NTT Japan, Japan
Roger Oyono	Université de la Polynésie Française
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Vincent Rijmen	Technische Universität Graz, Austria
Francesco Sica (Co-chair)	AceCrypt – Mount Allison University, Canada
Doug Stinson	University of Waterloo, Canada

Nicolas Thériault
Michael Wiener
Adam Young
Amr Youssef

Universidad de Talca, Chile
Cryptographic Clarity, Canada
MITRE Corp, USA
Concordia University, Canada

External Reviewers

Tolga Acar
Laila El Aïmani
Davide Alessio
Elena Andreeva
Kazumaro Aoki
Frederik Armknecht
Gilles Van Assche
Jean-Claude Bajard
Côme Berbain
Thierry Berger
Daniel J. Bernstein
and Tanja Lange
Andrey Bogdanov
Guilhem Castagnos
Li Chao
Pierre-Louis Cayrel
Jean-Sébastien Coron
Nicolas Courtois
Joan Daemen
Jérémy Detrey
Vassil Dimitrov
Yevgeniy Dodis
Thomas Dullien
Matthieu Finiasz
Ewan Fleischmann
Pierre-Alain Fouque
Julien Francq
Benedikt Gierlichs
Guang Gong
Michael Gorski
Louis Granboulan
Johann Großschädl
Sylvain Guilley
Tim Güneysu
Helena Handschuh
Darrel Hankerson
Martin Hell

Peter Hellekalek
Kevin Henry
Miia Hermelin
Mathias Herrmann
Sebastian Indesteege
Tetsu Iwata
Thomas Johansson
Pascal Junod
Timo Kasper
Ulrich Kühn
Alexandre Karlov
Shahram Khazaei
Aleksandar Kircanski
Patrick Lacharme
Mario Lamberger
Kerstin Lemke-Rust
Gaëtan Leurent
Benoît Libert
Daniel Loebenberger
Subhamoy Maitra
Stéphane Manuel
Kerry McKay
Willi Meier
Florian Mendel
Alfred Menezes
Tomislav Nad
Mridul Nandi
Christophe Negre
Michael Nüsken
Katsuyuki Okeya
Francis Olivier
Siddika Berna Örs
Onur Özen
Dan Page
Jacques Patarin
Maura Paterson
Josef Pieprzyk

Axel Poschmann
Emmanuel Prouff
Michael Quisquater
Håvard Raddum
Christian Rechberger
Tom Ristenpart
Christophe Ritzenthaler
Matt Robshaw
Robert Rolland
Neyire Deniz Sarier
Juraj Sarinay
Palash Sarkar
Martin Schlaeffer
Peter Schwabe
Taizo Shirai
Igor Shparlinski
Hervé Sibert
Andrey Sidorenko
Martijn Stam
François-Xavier
Standaert
Dirk Stegemann
Ron Steinfeld
Marc Stevens
Christine Swart
Stefano Tessaro
Arnaud Tisserand
Yukiyasu Tsunoo
Berkant Ustaoglu
Frederik Vercauteren
Damien Vergnaud
Jiang Wu
Brecht Wyseur
Jens Zumbärgel

Table of Contents

Elliptic and Hyperelliptic Curve Arithmetic

Faster Halvings in Genus 2	1
<i>Peter Birkner and Nicolas Thériault</i>	
Efficient Pairing Computation on Genus 2 Curves in Projective Coordinates	18
<i>Xinxin Fan, Guang Gong, and David Jao</i>	
On Software Parallel Implementation of Cryptographic Pairings	35
<i>Philipp Grabher, Johann Großschädl, and Dan Page</i>	

Block Ciphers I

The Cryptanalysis of Reduced-Round SMS4	51
<i>Jonathan Etrog and Matt J.B. Robshaw</i>	
Building Secure Block Ciphers on Generic Attacks Assumptions	66
<i>Jacques Patarin and Yannick Seurin</i>	

First Invited Talk

Lifting and Elliptic Curve Discrete Logarithms	82
<i>Joseph H. Silverman</i>	

Hash Functions I

Preimage Attacks on One-Block MD4, 63-Step MD5 and More	103
<i>Kazumaro Aoki and Yu Sasaki</i>	
Preimage Attacks on 3-Pass HAVAL and Step-Reduced MD5	120
<i>Jean-Philippe Aumasson, Willi Meier, and Florian Mendel</i>	
Cryptanalysis of Tweaked Versions of SMASH and Reparation	136
<i>Pierre-Alain Fouque, Jacques Stern, and Sébastien Zimmer</i>	

Mathematical Aspects of Applied Cryptography I

Counting Functions for the k -Error Linear Complexity of 2^n -Periodic Binary Sequences	151
<i>Ramakanth Kavuluru and Andrew Klapper</i>	
On the Exact Success Rate of Side Channel Analysis in the Gaussian Model	165
<i>Matthieu Rivain</i>	

Stream Ciphers Cryptanalysis

Algebraic and Correlation Attacks against Linearly Filtered Non Linear Feedback Shift Registers	184
<i>Côme Berbain, Henri Gilbert, and Antoine Joux</i>	
A Cache Timing Analysis of HC-256	199
<i>Erik Zenner</i>	
An Improved Fast Correlation Attack on Stream Ciphers	214
<i>Bin Zhang and Dengguo Feng</i>	

Hash Functions II

A Three-Property-Secure Hash Function	228
<i>Elena Andreeva and Bart Preneel</i>	
Analysis of the Collision Resistance of RadioGatún Using Algebraic Techniques	245
<i>Charles Bouillaguet and Pierre-Alain Fouque</i>	
A Scheme to Base a Hash Function on a Block Cipher	262
<i>Shoichi Hirose and Hidenori Kuwakado</i>	
Collisions and Other Non-random Properties for Step-Reduced SHA-256	276
<i>Sebastiaan Indestege, Florian Mendel, Bart Preneel, and Christian Rechberger</i>	

Cryptography with Algebraic Curves

Public Verifiability from Pairings in Secret Sharing Schemes	294
<i>Somayeh Heidarvand and Jorge L. Villar</i>	

The Elliptic Curve Discrete Logarithm Problem and Equivalent Hard Problems for Elliptic Divisibility Sequences	309
<i>Kristin E. Lauter and Katherine E. Stange</i>	

Second Invited Talk – Stafford Tavares Lecture

The “Coefficients H” Technique	328
<i>Jacques Patarin</i>	

Mathematical Aspects of Applied Cryptography II

Distinguishing Multiplications from Squaring Operations	346
<i>Frederic Amiel, Benoit Feix, Michael Tunstall, Claire Whelan, and William P. Marnane</i>	
Subquadratic Polynomial Multiplication over $GF(2^m)$ Using Trinomial Bases and Chinese Remaindering	361
<i>Éric Schost and Arash Hariri</i>	
Bounds on Fixed Input/Output Length Post-processing Functions for Biased Physical Random Number Generators	373
<i>Kyohei Suzuki and Tetsu Iwata</i>	

Curve-Based Primitives in Hardware

HECC Goes Embedded: An Area-Efficient Implementation of HECC . . .	387
<i>Junfeng Fan, Lejla Batina, and Ingrid Verbauwhede</i>	
ECC Is Ready for RFID – A Proof in Silicon	401
<i>Daniel Hein, Johannes Wolkerstorfer, and Norbert Felber</i>	

Block Ciphers II

Cryptanalysis of a Generic Class of White-Box Implementations	414
<i>Wil Michiels, Paul Gorissen, and Henk D.L. Hollmann</i>	
New Linear Cryptanalytic Results of Reduced-Round of CAST-128 and CAST-256	429
<i>Meiqin Wang, Xiaoyun Wang, and Changhui Hu</i>	
Improved Impossible Differential Cryptanalysis of Reduced-Round Camellia	442
<i>Wenling Wu, Lei Zhang, and Wentao Zhang</i>	
Author Index	457