Lecture Notes in Computer Science 5381

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer

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



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 through 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 Polynesie 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 | Universidad de Talca, Chile |
| Michael Wiener | Cryptographic Clarity, Canada |
| Adam Young | MITRE Corp, USA |
| Amr Youssef | Concordia University, Canada |

## External Reviewers

Tolga Acar
Laila El Aimani
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
Jérémie 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
Sebastiaan 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
Sıddıka 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 Ustoaglu
Frederik Vercauteren
Damien Vergnaud
Jiang Wu
Brecht Wyseur
Jens Zumbrägel

# Table of Contents

## Elliptic and Hyperelliptic Curve Arithmetic



## Block Ciphers I



## First Invited Talk



## Hash Functions I

## Mathematical Aspects of Applied Cryptography I



## Stream Ciphers Cryptanalysis



## Hash Functions II



## Cryptography with Algebraic Curves

## Second Invited Talk – Stafford Tavares Lecture



## Mathematical Aspects of Applied Cryptography II



## Curve-Based Primitives in Hardware



## Block Ciphers II