

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

Michael J. Jacobson Jr. Vincent Rijmen
Reihaneh Safavi-Naini (Eds.)

Selected Areas in Cryptography

16th Annual International Workshop, SAC 2009
Calgary, Alberta, Canada, August 13-14, 2009
Revised Selected Papers

Volume Editors

Michael J. Jacobson Jr.

University of Calgary, Department of Computer Science
2500 University Drive NW, Calgary, Alberta, T2N 1N4, Canada
E-mail: jacobs@cpsc.ucalgary.ca

Vincent Rijmen

K.U. Leuven, ESAT/COSIC
Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium
E-mail: vincent.rijmen@esat.kuleuven.be

Reihaneh Safavi-Naini

University of Calgary, Department of Computer Science
2500 University Drive NW, Calgary, Alberta, T2N 1N4, Canada
E-mail: rei@ucalgary.ca

Library of Congress Control Number: 2009937877

CR Subject Classification (1998): E.3, K.6.5, D.4.6, E.2, K.4.4, I.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-642-05443-9 Springer Berlin Heidelberg New York

ISBN-13 978-3-642-05443-3 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: 12788668 06/3180 5 4 3 2 1 0

Preface

The 16th Workshop on Selected Areas in Cryptography (SAC 2009) was held at the University of Calgary, in Calgary, Alberta, Canada, during August 13-14, 2009. There were 74 participants from 19 countries. Previous workshops in this series were held at Queens 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), Concordia University in Montreal (2006), University of Ottawa (2007), and Mount Allison University in Sackville (2008).

The themes for SAC 2009 were:

1. Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, and MAC algorithms
2. Efficient implementations of symmetric and public key algorithms
3. Mathematical and algorithmic aspects of applied cryptology
4. Privacy enhancing cryptographic systems

This included the traditional themes (the first three) together with a special theme for 2009 workshop (fourth theme).

We received 86 submissions, of which one was withdrawn. The review was double-blinded. Each paper was reviewed by three members of the Program Committee and submissions that were co-authored by a member of Program Committee received two additional reviews. No member of Program Committee reviewed their own submission. The average quality of submissions was high and this made final selection of the papers a challenging task. We accepted 28 papers with 10 papers in the area of hash functions. The high number of papers in this area could be partially attributed to the interest generated in this area by the NIST competition. The remaining 18 papers were on block and stream ciphers, public key schemes, implementation, and privacy-enhancing cryptographic systems.

In addition, the program included two invited talks:

- Jan Camenisch — Privacy-Enhancing Cryptography: Theory and Practice
- Andreas Enge — Elliptic Complex Multiplication in Cryptography

We would like to thank the Program Committee for their hard work and careful reviews. We also benefited from the expertise of many external reviewers who helped the Program Committee with high-quality reviews. A list of all external referees appears here.

We also would like to thank Coral Burns and Elmar Tischhauser for technical support, and Hadi Ahmadi, Mina Askari, Martin Gagné, Kris Narayan, Arthur Schmidt, Michal Sramka, and Mohammed Tuhin, whose effort ensured smooth running of the workshop.

Finally, we gratefully acknowledge the generous support of the Faculty of Science and Department of Computer Science of the University of Calgary, the University of Calgary University Research Grants Committee, the informatics Circle of Research Excellence (iCORE), the Pacific Institute for the Mathematical Sciences (PIMS), and Microsoft Research for their generous financial support.

September 2009

Michael J. Jacobson, Jr.
Vincent Rijmen
Reihaneh Safavi-Naini

16th Annual Workshop on Selected Areas in Cryptography

August 13–14, 2007, Calgary, Alberta, Canada

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

Conference Co-chairs

| | |
|--------------------------|---|
| Michael J. Jacobson, Jr. | University of Calgary, Canada |
| Vincent Rijmen | Katholieke Universiteit Leuven, Belgium and Graz University of Technology, Austria |
| Reihaneh Safavi-Naini | University of Calgary, Canada |

Program Committee

| | |
|--------------------|---|
| Masayuki Abe | NTT, Japan |
| Mikhail J. Atallah | Purdue University, USA |
| Roberto Avanzi | Ruhr University Bochum, Germany |
| Feng Bao | Institute for Infocomm Research, Singapore |
| Paulo Barreto | University of São Paulo, Brazil |
| Jan Camenisch | IBM Research, Switzerland |
| Vassil Dimitrov | University of Calgary, Canada |
| Christophe Doche | Macquarie University, Australia |
| Orr Dunkelman | Ecole Normale Supérieure, France |
| Helena Handschuh | Katholieke Universiteit Leuven, Belgium |
| Thomas Johansson | Lund University, Sweden |
| Mike Just | University of Edinburgh, UK |
| Charanjit Jutla | IBM Research, USA |
| Liam Keliher | Mount Allison University, Canada |
| Xuejia Lai | Shanghai Jiao Tong University, PR China |
| Pil Jong Lee | Pohang University of Science and Technology, Korea |
| Mitsuru Matsui | Mitsubishi Electric Corporation, Japan |
| Shiho Moriai | Sony Corporation, Japan |
| Eiji Okamoto | University of Tsukuba, Japan |
| Josef Pieprzyk | Macquarie University, Australia |
| Bart Preneel | Katholieke Universiteit Leuven, Belgium |
| Matt Robshaw | Orange Labs, France |
| Francesco Sica | |
| Doug Stinson | University of Waterloo, Canada |
| Edlyn Teske | University of Waterloo, Canada |

Nicolas Thériault
Adam L. Young
Amr Youssef
Michael Wiener

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

External Reviewers

Martin Ågren
Toru Akishita
Elena Andreeva
Kazumaro Aoki
Adem Atalay
Dan Bernstein
Marina Blanton
Charles Bouillaguet
Suresh Chari
Joo Yeon Cho
Ming Duan
Sung Wook Eom
Keith Frikken
Philippe Gaborit
Willi Geiselmann
Darrel Hankerson
Nadia Heninger
Florian Hess
Howard Heys
Seok Hee Hong
Marko Hölbl
Sebastiaan Indestege
Kimmo Jarvinen
Marcos A. Simplicio Jr.
Anindya Patthak
Nathan Keller
Sun Young Kim
Kazukuni Kobara
Dae Sung Kwon
Tanja Lange
Gaëtan Leurent
Ji Li
Wei Li
Julio Lopez
Stefan Lucks
Yiyuan Luo
Alex May
Nicky Mouha

Michael Naehrig
Anderson Clayton Nascimento
Maria Naya-Plasencia
Mehrdad Nojoumian
Raphael C.-W. Phan
Daniel Rasmussen
Thomas Ristenpart
Andy Rupp
Yu Sasaki
Michael Scott
Yannick Seurin
Igor Shparlinski
Paul Stankovski
Ron Steinfeld
Jiayuan Sui
Xiaorui Sun
Daisuke Suzuki
Koutarou Suzuki
Elmar Tischhauser
Jalaj Upadhyay
Berkant Ustaoglu
Salil Vadhan
Vesselin Velichkov
Frederik Vercauteren
Huaxiong Wang
Yongtao Wang
Ruizhong Wei
Jian Weng
Hongjun Wu
Jiang Wu
Zhongming Wu
Liangyu Xu
Kan Yasuda
Muhammad Reza Z'Abab
Greg Zaverucha
Erik Zenner
Bo Zhu

Sponsoring Institutions

The Faculty of Science and Department of Computer Science of the University of Calgary

The University of Calgary University Research Grants Committee

The informatics Circle of Research Excellence (iCORE)

The Pacific Institute for the Mathematical Sciences (PIMS)

Microsoft Research

Table of Contents

Hash Functions I

| | |
|---|----|
| Practical Collisions for SHAMATA-256 | 1 |
| <i>Sebastian Indestege, Florian Mendel, Bart Preneel, and Martin Schl affer</i> | |
| Improved Cryptanalysis of the Reduced Gr stl Compression Function, ECHO Permutation and AES Block Cipher | 16 |
| <i>Florian Mendel, Thomas Peyrin, Christian Rechberger, and Martin Schl affer</i> | |
| Cryptanalyses of Narrow-Pipe Mode of Operation in AURORA-512 Hash Function | 36 |
| <i>Yu Sasaki</i> | |

Miscellaneous Techniques

| | |
|---|----|
| More on Key Wrapping | 53 |
| <i>Rosario Gennaro and Shai Halevi</i> | |
| Information Theoretically Secure Multi Party Set Intersection Re-visited | 71 |
| <i>Arpita Patra, Ashish Choudhary, and C. Pandu Rangan</i> | |
| Real Traceable Signatures | 92 |
| <i>Sherman S.M. Chow</i> | |

Hash Functions II

| | |
|---|-----|
| Cryptanalysis of Hash Functions with Structures | 108 |
| <i>Dmitry Khovratovich</i> | |
| Cryptanalysis of the LANE Hash Function | 126 |
| <i>Shuang Wu, Denguo Feng, and Wenling Wu</i> | |
| Practical Pseudo-collisions for Hash Functions ARIRANG-224/384 | 141 |
| <i>Jian Guo, Krystian Matusiewicz, Lars R. Knudsen, San Ling, and Huaxiong Wang</i> | |

Hardware Implementation and Cryptanalysis

| | |
|--|-----|
| A More Compact AES | 157 |
| <i>David Canright and Dag Arne Osvik</i> | |

Optimization Strategies for Hardware-Based Cofactorization 170
Daniel Loebenberger and Jens Putzka

More on the Security of Linear RFID Authentication Protocols 182
Matthias Krause and Dirk Stegemann

Differential Fault Analysis of Rabbit 197
Aleksandar Kircanski and Amr M. Youssef

An Improved Recovery Algorithm for Decayed AES Key Schedule
 Images 215
Alex Tsow

Block Ciphers

Cryptanalysis of the Full MMB Block Cipher 231
Meiqin Wang, Jorge Nakahara Jr., and Yue Sun

Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis 249
Kenji Ohkuma

Improved Integral Attacks on MISTY1 266
Xiaorui Sun and Xuejia Lai

New Results on Impossible Differential Cryptanalysis of
 Reduced-Round Camellia-128 281
*Hamid Mala, Mohsen Shakiba, Mohammad Dakhilalian, and
 Ghadamali Bagherikaram*

Modes of Operation

Format-Preserving Encryption 295
Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, and Till Stegers

BTM: A Single-Key, Inverse-Cipher-Free Mode for Deterministic
 Authenticated Encryption 313
Tetsu Iwata and Kan Yasuda

Implementation of Public Key Cryptography

On Repeated Squarings in Binary Fields 331
Kimmo U. Järvinen

Highly Regular m -Ary Powering Ladders 350
Marc Joye

An Efficient Residue Group Multiplication for the η_T Pairing over
 \mathbb{F}_{3^m} 364
Yuta Sasaki, Satsuki Nishina, Masaaki Shirase, and Tsuyoshi Takagi

| | |
|--|-----|
| Compact McEliece Keys from Goppa Codes | 376 |
| <i>Rafael Misoczki and Paulo S.L.M. Barreto</i> | |

Hash Functions and Stream Ciphers

| | |
|---|-----|
| Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damgård | 393 |
| <i>Elena Andreeva, Charles Bouillaguet, Orr Dunkelman, and John Kelsey</i> | |
| Cryptanalysis of Dynamic SHA(2) | 415 |
| <i>Jean-Philippe Aumasson, Orr Dunkelman, Sebastiaan Indestege, and Bart Preneel</i> | |
| A New Approach for FCSRs | 433 |
| <i>François Arnault, Thierry Berger, Cédric Lauradoux, Marine Minier, and Benjamin Pousse</i> | |
| New Cryptanalysis of Irregularly Decimated Stream Ciphers | 449 |
| <i>Bin Zhang</i> | |
| Author Index | 467 |