

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

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

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Eli Biham Amr M. Youssef (Eds.)

Selected Areas in Cryptography

13th International Workshop, SAC 2006
Montreal, Canada, August 17-18, 2006
Revised Selected Papers

Volume Editors

Eli Biham

Technion - Israel Institute of Technology

Computer Science Department

Haifa 32000, Israel

E-mail: biham@cs.technion.ac.il

Amr M. Youssef

Concordia University

Concordia Institute for Information Systems Engineering

1425 René Lévesque Blvd. West, Montreal, Quebec, H3G 1M8, Canada

E-mail: youssef@ciise.concordia.ca

Library of Congress Control Number: 2007935809

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 3-540-74461-4 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-74461-0 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: 12111787 06/3180 5 4 3 2 1 0

Preface

These are the proceedings of SAC 2006, the thirteenth annual workshop on Selected Areas in Cryptography. The workshop was sponsored by the Concordia Institute for Information Systems Engineering, in cooperation with the IACR, the International Association of Cryptologic Research, www.iacr.org. This year's themes for SAC were:

1. Design and analysis of symmetric key cryptosystems
2. Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms
3. Efficient implementations of symmetric and public key algorithms
4. Side-channel analysis (DPA, DFA, Cache analysis, etc.)

A total of 25 papers were accepted for presentation at the workshop, out of 86 papers submitted (of which one was withdrawn by the authors shortly after the submission deadline). These proceedings contain revised versions of the accepted papers. In addition two invited talks were given: Adi Shamir gave the Stafford Tavares Lecture, entitled "A Top View of Side Channels". The second invited talk was given by Serge Vaudenay entitled "When Stream Cipher Analysis Meets Public-Key Cryptography" (his paper on this topic is enclosed in these proceedings).

The reviewing process was a challenging task, and many good submissions had to be rejected. Each paper was reviewed by at least three members of the Program Committee, and papers co-authored by a member of the Program Committee were reviewed by at least five (other) members. The reviews were then followed by deep discussions on the papers, which contributed a lot to the quality of the final selection. In most cases, extensive comments were sent to the authors. A total of about 300 reviews were written by the committee and external reviewers for the 86 papers, of which 92 reviews were made by 65 external reviewers. Over 240 discussion comments were made by committee members (with up to 30 comments per member). Several papers had deep discussions with 17–19 discussion comments each. In addition, the Co-chairs wrote over 200 additional discussion comments.

It was a pleasure for us to work with the Program Committee, whose members worked very hard during the review process. We are also very grateful to the external referees, who contributed with their special expertise to the selection process. Their work is highly appreciated.

The submission and review process was done using an electronic submission and review software written by Thomas Baignères and Matthieu Finiasz. Thomas and Matthieu also modified and improved their system especially for SAC 2006, with many new features. Their response was very quick and timely, and in many cases features were added or changes were made within less than an hour. We wish to thank them very much for all this work.

We would also like to acknowledge Sheryl Tablan and Sheila Anderson for their great help in the local organization.

Finally, but most importantly, we would like to thank all the authors from all over the world who submitted papers to the workshop, and to all the participants at the workshop.

October 2006

Eli Biham
Amr Youssef

SAC 2006

August 17–18, 2006, Montréal, Canada

Sponsored by the
Concordia Institute for Information Systems Engineering

In cooperation with the
International Association of Cryptologic Research (IACR)

Workshop Co-chairs

Eli Biham, Computer Science Department, Technion – Israel
Institute of Technology, Technion City, Haifa 32000, Israel

Amr M. Youssef, Concordia Institute for Information Systems
Engineering, Concordia University, 1425 René Lévesque Blvd.
West, Montréal, Quebec, H3G 1T7, Canada

Program Committee

Carlisle Adams..... University of Ottawa, Canada
Alex Biryukov University of Luxembourg, Luxembourg
Nicolas Courtois..... Axalto, France
Orr Dunkelman Technion, Israel
Helena Handschuh Spansion, EMEA, France
Thomas Johansson..... Lund, Sweden
Antoine Joux Université de Versailles St-Quentin-en-Yvelines, France
Pascal Junod Nagravision, Switzerland
Lars Knudsen DTU, Denmark
Stefan Lucks University of Mannheim, Germany
Bart Preneel..... Katholieke Universiteit Leuven, Belgium
Matt Robshaw France Telecom, France
Doug Stinson..... University of Waterloo, Canada
Stafford Tavares..... Queen's University, Canada
Eran Tromer..... Weizmann Institute of Science, Israel
Xiaoyun Wang..... Tsinghua University and Shandong University, China
Michael Wiener Cryptographic Clarity, Canada

External Referees

Frederik Armknecht
Thomas Baignères
Elad Barkan
Lejla Batina
Aurélie Bauer
Come Berbain
Johannes Bloemer
Colin Boyd
Anne Canteaut
Rafi Chen
Carlos Cid
Jeremy Clark
Scott Contini
Ivan Damgaard
Blandine Debraize
Håkan Englund
Aleks Essex
Matthieu Finiasz
Ewan Fleischmann
Guillaume Fumaroli
Henri Gilbert
Martin Hell

Matt Henricksen
Jonathan J. Hoch
Tetsu Iwata
Ulrich Kühn
Nathan Keller
Matthias Krause
Simon Künzli
Tanja Lange
Joe Lano
Stefan Mangard
Alexander Maximov
Alexander May
Alfred Menezes
Nele Mentens
Brad Metz
Marine Minier
Jean Monnerat
James Muir
Sean Murphy
Mridul Nandi
Gregory Neven
Dag Arne Osvik

Pascal Paillier
Souradyuti Paul
Jan Pelzl
Gilles Piret
Axel Poschmann
Soren S. Thomsen
Kazuo Sakiyama
Kai Schramm
Jean-Pierre Seifert
Nigel Smart
Heiko Stamer
François-Xavier Standaert
Dirk Stegemann
Emin Tatli
Nicolas Theriault
Boaz Tsaban
Ingrid Verbauwhede
Frederik Vercauteren
Charlotte Vikkelsoe
Christopher Wolf
Robert Zuccherato

Table of Contents

Block Cipher Cryptanalysis

Improved DST Cryptanalysis of IDEA	1
<i>Eyüp Serdar Ayaz and Ali Aydın Selçuk</i>	
Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192	15
<i>Wentao Zhang, Wenling Wu, Lei Zhang, and Dengguo Feng</i>	
Related-Key Rectangle Attack on the Full SHACAL-1	28
<i>Orr Dunkelman, Nathan Keller, and Jongsung Kim</i>	

Stream Cipher Cryptanalysis I

Cryptanalysis of Achterbahn-Version 2	45
<i>Martin Hell and Thomas Johansson</i>	
Cryptanalysis of the Stream Cipher ABC v2	56
<i>Hongjun Wu and Bart Preneel</i>	

Block and Stream Ciphers

The Design of a Stream Cipher LEX	67
<i>Alex Biryukov</i>	
Dial C for Cipher	76
<i>Thomas Baignères and Matthieu Finiasz</i>	
Improved Security Analysis of XEX and LRW Modes	96
<i>Kazuhiko Minematsu</i>	

Side-Channel Attacks

Extended Hidden Number Problem and Its Cryptanalytic Applications	114
<i>Martin Hlaváč and Tomáš Rosa</i>	
Changing the Odds Against Masked Logic	134
<i>Kris Tiri and Patrick Schaumont</i>	
Advances on Access-Driven Cache Attacks on AES	147
<i>Michael Neve and Jean-Pierre Seifert</i>	

Blind Differential Cryptanalysis for Enhanced Power Attacks 163
Helena Handschuh and Bart Preneel

Efficient Implementations I

Efficient Implementations of Multivariate Quadratic Systems 174
Côme Berbain, Olivier Billet, and Henri Gilbert

Unbridle the Bit-Length of a Crypto-coprocessor with Montgomery
 Multiplication 188
Masayuki Yoshino, Katsuyuki Okeya, and Camille Vuillaume

Delaying and Merging Operations in Scalar Multiplication: Applications
 to Curve-Based Cryptosystems 203
Roberto Maria Avanzi

Stream Cipher Cryptanalysis II

On the Problem of Finding Linear Approximations and Cryptanalysis
 of Pomaranch Version 2 220
Martin Hell and Thomas Johansson

Multi-pass Fast Correlation Attack on Stream Ciphers 234
Bin Zhang and Dengguo Feng

Crossword Puzzle Attack on NLS 249
Joo Yeon Cho and Josef Pieprzyk

Invited Talk

When Stream Cipher Analysis Meets Public-Key Cryptography 266
Matthieu Finiasz and Serge Vaudenay

Efficient Implementations II

On Redundant τ -Adic Expansions and Non-adjacent Digit Sets 285
Roberto Maria Avanzi, Clemens Heuberger, and Helmut Prodinger

Pairing Calculation on Supersingular Genus 2 Curves 302
Colm Ó hÉigartaigh and Michael Scott

Efficient Divisor Class Halving on Genus Two Curves 317
Peter Birkner

Message Authentication Codes

Message Authentication on 64-Bit Architectures 327
Ted Krovetz

Some Notes on the Security of the Timed Efficient Stream Loss-Tolerant Authentication Scheme	342
<i>Goce Jakimoski</i>	

Hash Functions

Constructing an Ideal Hash Function from Weak Ideal Compression Functions	358
<i>Moses Liskov</i>	

Provably Good Codes for Hash Function Design	376
<i>Charanjit S. Jutla and Anindya C. Patthak</i>	

Author Index	395
---------------------------	-----