Lecture Notes in Computer Science 4356

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

Eli Biham Amr M. Youssef (Eds.)

Selected Areas in Cryptography

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

Springer

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

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A total of 25 papers were accepted for presentation at the workshop, out of 86 papers submitted (of which one was withdrawn by the authors shortly after the submission deadline).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

Efficient Implementations I

Stream Cipher Cryptanalysis II

Invited Talk

Efficient Implementations II

Message Authentication Codes

Hash Functions