Lecture Notes in Computer Science 11349

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

More information about this series at http://www.springer.com/series/7410

Carlos Cid · Michael J. Jacobson, Jr. (Eds.)

Selected Areas in Cryptography – SAC 2018

25th International Conference
Calgary, AB, Canada, August 15–17, 2018
Revised Selected Papers

Springer

Editors

Carlos Cid
Royal Holloway, University of London
Egham, UK

Michael J. Jacobson, Jr.
University of Calgary
Calgary, AB, Canada

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-10969-1 ISBN 978-3-030-10970-7 (eBook)
https://doi.org/10.1007/978-3-030-10970-7

Library of Congress Control Number: 2018965923

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The Conference on Selected Areas in Cryptography (SAC) is the leading Canadian venue for the presentation and publication of cryptographic research, and has been held annually since 1994. SAC celebrated its 25th anniversary in 2018, taking place for the second time at the University of Calgary in Calgary, Alberta. In keeping with its tradition, SAC 2018 offered a relaxed and collegial atmosphere for researchers to present and discuss new results.

There are four areas covered at each SAC conference. Three of them are permanent:

- Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes
- Efficient implementations of symmetric and public key algorithms
- Mathematical and algorithmic aspects of applied cryptology

A fourth area varies from year to year, and the special selected topic for SAC 2018 was “Cryptography for the Internet of Things.”

SAC 2018 received a total of 57 submissions, out of which the Program Committee (PC) selected 22 papers for presentation. The review process was thorough, with each submission receiving the attention of at least three reviewers (at least four for submissions involving a PC member). We would like to thank all authors for their submissions, and are very grateful to the PC members and reviewers for their effort and contribution to the selection of a high-quality program for SAC 2018.

There were three invited talks. The Stafford Tavares Lecture was given by Adi Shamir, who presented “Machine Learning in Security: Applications and Implications.” The second invited talk was given by Andrey Bogdanov, who spoke about “Whitebox Cryptography.” This year, in honor of its 25th anniversary, SAC had a special third invited talk by Carlisle Adams, who presented “SAC^{25}: A Retrospective.” Stafford Tavares, one of the co-founders of SAC, was also a special invited guest, and gave a retrospective presentation of SAC at the conference banquet.

This year SAC also hosted what is now the fourth iteration of the SAC Summer School (S3). S3 is intended to be a place where early-career researchers can increase their knowledge of cryptography through instruction by, and interaction with, leading researchers in the field. We were fortunate to have Daniel J. Bernstein (Cryptographic Software Engineering), Andrey Bogdanov (Design of Lightweight Symmetric-Key Algorithms), Francesco Regazzoni (Cryptographic Hardware Engineering), and Meltem Sonmez Turan (Applications and Standardization of Lightweight Cryptography). We would like to express our sincere gratitude to these four presenters for dedicating their time and effort to what has become a highly anticipated and highly beneficial event for all participants.

A special thanks also goes to the team at the University of Calgary Conference Services, our technical and administrative support (Coral Burns, Mitra Mottaghi, and

Humaira Waqar), and our local student volunteers (Sepideh Avizheh, Shuai Li, Simpy Parveen, and Randy Yee) for their tireless support to the organisation of SAC 2018, both before and during the conference. Finally, we are very grateful to our sponsors, the Communications Security Establishment, Alberta Innovates, the Institute for Security, Privacy and Information Assurance, the Pacific Institute for the Mathematical Sciences, Springer, and the University of Calgary's Department of Computer Science, Faculty of Science, and Office of the Vice-President (Research), whose enthusiastic support (both financial and otherwise) greatly contributed to the success of SAC 2018.

November 2018

Carlos Cid
Michael J. Jacobson, Jr.

Organization

General and Program Chairs

Carlos Cid	Royal Holloway University of London, UK
Michael J. Jacobson, Jr.	University of Calgary, Canada

Program Committee

Carlisle Adams	University of Ottawa, Canada
Diego Aranha	University of Campinas, Brazil
Frederik Armknecht	Universität Mannheim, Germany
Roberto Avanzi	ARM, Germany
Steve Babbage	Vodafone, UK
Paulo Barreto	University of Washington Tacoma, USA
Daniel J. Bernstein	University of Illinois at Chicago, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Andrey Bogdanov	DTU, Denmark
Vassil Dimitrov	University of Calgary, Canada
Itai Dinur	Ben-Gurion University, Israel
Maria Eichlseder	TU Graz, Austria
Pierre-Alain Fouque	Université Rennes and Institut Universitaire de France, France
Guang Gong	University of Waterloo, Canada
Johann Groszschaedl	University of Luxembourg, Luxembourg
M. Anwar Hasan	University of Waterloo, Canada
Howard Heys	Memorial University of Newfoundland, Canada
Jérémy Jean	ANSSI, France
Elif Bilge Kavun	Infineon Technologies, Germany
Stefan Kölbl	DTU, Denmark
Gaëtan Leurent	Inria, France
Subhamoy Maitra	Indian Statistical Institute, India
Brice Minaud	Royal Holloway University of London, UK
Nicky Mouha	NIST, USA
Michael Naehrig	Microsoft Research, USA
Svetla Nikova	KU Leuven, Belgium
Ludovic Perret	Sorbonne University/Inria/CNRS, France
Josef Pieprzyk	Data61, CSIRO, Australia
Francesco Regazzoni	Università della Svizzera Italiana, Switzerland
Matt Robshaw	Impinj, USA
Sondre Rønjom	University of Bergen, Norway
Fabrizio De Santis	Siemens AG, Germany
Sujoy Sinha Roy	KU Leuven, Belgium

Jörn-Marc Schmidt	secunet Security Networks, Germany
Peter Schwabe	Radboud University, The Netherlands
Kyoji Shibutani	Sony Corporation, Japan
Paul Stankovski	Lund University, Sweden
Frederik Vercauteren	KU Leuven, Belgium
Meiqin Wang	Shandong University, China
Hongjun Wu	Nanyang Technological University, Singapore
Huapeng Wu	University of Windsor, Canada
Bo-Yin Yang	Academia Sinica, Taiwan
Kan Yasuda	NTT, Japan
Amr Youssef	Concordia University, Canada

Additional Reviewers

Josep Balasch
Ward Beullens
Wouter Castryck
Morten Dahl
Jan-Pieter D'Anvers
Lauren De Meyer
Sébastien Duval
Wieland Fischer
Benedikt Gierlichs
Florian Goepfert
Angela Jäschke
Tanja Lange
Erik Mårtensson
Rachel Player
Vincent Rijmen
Hermann Seuschek
Alan Szepieniec
Zhenfei Zhang

Contents

Design of Symmetric Key Primitives

Cryptanalysis of Symmetric Key Primitives

Side Channel and Fault Attacks

Post-Quantum Cryptography

Lattice-Based Cryptography

Classical Public Key Cryptography

Machine Learning and Cryptography