Lecture Notes in Computer Science 10831

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

Antoine Joux · Abderrahmane Nitaj
Tajjeeddine Rachidi (Eds.)

Progress in Cryptology – AFRICACRYPT 2018

10th International Conference on Cryptology in Africa
Marrakesh, Morocco, May 7–9, 2018
Proceedings

Springer

Editors
Antoine Joux
Fondation Partenariale de Sorbonne Université
Paris
France

Abderrahmane Nitaj
Université de Caen
Caen
France

Tajjeeddine Rachidi
Al Akhawayn University
Ifrane
Morocco

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-89338-9 ISBN 978-3-319-89339-6 (eBook)
https://doi.org/10.1007/978-3-319-89339-6

Library of Congress Control Number: 2018937402

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

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

Preface

AFRICACRYPT 2018, the 10th International Conference on the Theory and Application of Cryptographic Techniques in Africa, took place in Marrakesh, Morocco, May 7–9, 2018. The conference was organized by Al Akhawayn University in Ifrane in cooperation with the International Association for Cryptologic Research (IACR).

The conference received a total of 54 submissions. Each submission was anonymized for the reviewing process and was assigned to three reviewers out of the 41 Program Committee members.

The Program Committee, aided by reports from 37 external reviewers, produced a total of 156 reviews. After highly interactive discussions and careful deliberation, the Program Committee selected 19 papers for presentation. The authors of accepted papers were given a week to prepare final versions of their papers for these proceedings. The revised versions of these papers are included in these proceedings and classified into two topics: symmetric cryptography and asymmetric cryptography.

The program was completed with two invited talks by Joan Daemen from Radboud University in Nijmegen, The Netherlands, and STMicroelectronics; and by Léo Ducas from CWI, Amsterdam, The Netherlands. We are very grateful to them for accepting our invitation.

We would like to thank all authors who submitted papers. The submissions came from: Australia, Austria, Belgium, Brazil, Canada, China, France, Germany, India, Iran, Japan, Morocco, Norway, Portugal, Romania, Senegal, Singapore, Sweden, Switzerland, Taiwan, The Netherlands, UAE, UK, and USA. We regret that the Program Committee rejected some very good papers. We know that this can be very disappointing. We sincerely hope that these works, eventually, get the attention they deserve elsewhere.

We are deeply grateful to the Program Committee and to the external reviewers for their hard work, enthusiasm, and conscientious efforts to ensure that each paper received a thorough and fair review.

We would also like to thank Springer for agreeing to an accelerated schedule for printing these proceedings, the EasyChair team for allowing us to use their platform, and Al Akhawayn University in Ifrane for supporting the conference.

We also thank the local Organizing Committee for their commitment and hard work to make the conference an enjoyable experience. We also thank Driss Ouaouicha and Kevin Smith, respectively, President and Dean of the School of Science and Engineering at Al Akhawayn University, for their financial and unconditional moral support. We extend our gratitude to the conference sponsors S2M Morocco for financially supporting the conference.

Last but not least, we thank everyone else, speakers, session chairs, and rump session chairs for their contribution to the program of Africacrypt 2018.

Finally, we wish to thank the participants and presenters. They all made Africacrypt 2018 a highly recognized forum for researchers to interact and share their works and knowledge with their peers, for the overall growth and development of cryptology research in the world and in Africa in particular.

May 2018

Antoine Joux
Abderrahmane Nitaj
Tajjeeddine Rachidi

Organization

Africacrypt 2018 was organized by Al Akhawayn University in Ifrane, Morocco.

General Chair

Tajjeeddine Rachidi	Al Akhawayn University in Ifrane, Morocco

Program Chairs

Antoine Joux	Fondation Partenariale de Sorbonne Université, IMJ-PRG, Paris, France
Abderrahmane Nitaj	University of Caen Normandie, France
Tajjeeddine Rachidi	Al Akhawayn University in Ifrane, Morocco

Organizing Committee

Latifa El Mortaji (Chair)	Al Akhawayn University, Ifrane, Morocco
Bouchra Saad	Al Akhawayn University, Ifrane, Morocco

Program Committee

Elena Andreeva	Katholieke Universiteit Leuven, Belgium
Hatem M. Bahig	Ain Shams University, Cairo, Egypt
Magali Bardet	University of Rouen, France
Hussain Benazza	University of Meknes, Morocco
Colin Boyd	Norwegian University of Science and Technology, Norway
Dario Catalano	Università di Catania, Italy
Xing Chaoping	Nanyang Technological University, Singapore
Sherman S. M. Chow	The Chinese University of Hong Kong, SAR China
Nicolas Courtois	University College London, UK
Luca De Feo	University de Versaille – Saint-Quentin-en-Yvelines, France
Milena Djukanovic	University of Montenegro
Nadia El Mrabet	SAS - CGCP - EMSE, France
Pierre-Alain Fouque	University of Rennes, France
Aline Gouget	Gemalto, France
Gottfried Herold	ENS Lyon, France
Javier Herranz	Universitat Politècnica de Catalunya, Spain
Hieuphan Duong	University of Limoges, France
Sorina Ionica	Université de Picardie, France

Tetsu Iwata	Nagoya University, Japan
Antoine Joux	Fondation Partenariale de Sorbonne Université, IMJ-PRG, Paris, France
Juliane Kramer	TU Darmstadt, Germany
Fabien Laguillaumie	University of Lyon I/LIP, France
Tancrède Lepoint	SRI International, USA
Abderrahmane Nitaj	University of Caen Normandie, France
Ayoub Otmani	University of Rouen Normandie, France
Elizabeth A. Quaglia	Royal Holloway, University of London, UK
Tajjeeddine Rachidi	Al Akhawayn University in Ifrane, Morocco
Adeline Roux-Langlois	CNRS-IRISA, France
Magdy Saeb	Arab Academy for Science, Technology Institute Maritime Transport, Alexandria, Egypt
Rei Safavi-Naini	University of Calgary, Canada
Palash Sarkar	Indian Statistical Institute, India
Alessandra Scafuro	North Carolina State University, Raleigh, USA
Peter Schwabe	Radboud University Nijmegen, The Netherlands
Djiby Sow	University of Dakar, Senegal
Pontelimon Stanica	Naval Postgraduate School, Monterey, USA
Noah Stephens-Davidowitz	New York University, USA
Willy Susilo	University of Wollongong, Australia
Joseph Tonien	University of Wollongong, Australia
Damien Vergnaud	Sorbonne Université, Paris, France
Vanessa Vitse	University of Grenoble, France
Amr M. Youssef	Concordia University, Canada

Additional Reviewers

Luca Nizzardo	Sumit Pandey	Subhadip Singha
Michael Walter	Nicolas Gama	Olivier Sanders
Ashley Fraser	Mohamed Elsheikh	Khoa Nguyen
Karim Bigou	Marine Minier	Fabrice Mouhartem
Guilherme Perin	Antoine Loiseau	Pierre Karpman
Sepideh Avizheh	Viet Cuong Trinh	Matteo Scarlata
Hisham Galal	Peter Spacek	Thomas De Cnudde
Mamun Akand	Julien Eynard	Paul Germouty
Sebati Ghosh	Kerem Varici	Brice Minaud
Yongjun Zhao	Valentin Suder	Sabyasachi Karati
Mohamed Tolba	Begül Bilgin	
Pauline Bert	Joan Daemen	

Invited Speakers

Joan Daemen	Radboud University in Nijmegen, The Netherlands, and STMicroelectronics
Léo Ducas	CWI, Amsterdam, The Netherlands

Sponsoring Institutions

Al Akhawayn University in Ifrane, Morocco
Société Maghrébine de Monétique (S2M), Morocco, http://www.s2m.ma

Contents