# Lecture Notes in Computer Science 10239

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

## Editorial Board

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

Marc Joye · Abderrahmane Nitaj (Eds.)

# Progress in Cryptology - AFRICACRYPT 2017

9th International Conference on Cryptology in Africa
Dakar, Senegal, May 24–26, 2017
Proceedings

Springer

*Editors*
Marc Joye
NXP Semiconductors
San Jose, CA
USA

Abderrahmane Nitaj
University of Caen
Caen
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-57338-0 ISBN 978-3-319-57339-7 (eBook)
DOI 10.1007/978-3-319-57339-7

Library of Congress Control Number: 2017937579

LNCS Sublibrary: SL4 – Security and Cryptology



Printed on acid-free paper

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

# Preface

The 9th International Conference on the Theory and Application of Cryptographic Techniques in Africa, Africacrypt 2017, took place May 24–26, 2017, in Dakar, Senegal. The conference was organized by Cheikh Anta Diop University, Dakar, Senegal, in cooperation with the International Association for Cryptologic Research (IACR). We heartily thank our general chairs, Mamadou Sangharé, Djiby Sow, and Abdoul Aziz Ciss, as well as the whole Organizing Committee for their efforts in making the conference a success.

The aim of Africacrypt is to provide an international forum for practitioners and researchers from industry, academia, and government from all over the world for a wide-ranging discussion of all forms of cryptography and its applications.

The conference received a total of 40 full papers, out of which 13 papers were selected for publication in these proceedings. Each submission was assigned at least three Program Committee (PC) members. In addition to the PC members, many external reviewers joined the review process in their particular areas of expertise. We were fortunate to have this energetic team of experts, and are deeply grateful to all of them for their hard work, which included a very active discussion phase. The paper submission, review, and discussion processes were effectively and efficiently made possible by the Web-based system developed by Shai Halevi. We thank him for his support and the IACR for hosting the review system. The program was completed with two keynote talks by Johannes Buchmann and Damien Stehlé, and by an invited talk by Luca De Feo. We are very grateful to them for accepting our invitation.

Last but not least, we would like to thank all the authors who submitted papers to this conference, the Organizing Committee members, colleagues, and student helpers for their valuable time and effort, and all the conference attendees who made this event a truly intellectually stimulating one through their active participation.

March 2017

Marc Joye
Abderrahmane Nitaj

# Organization

# AFRICACRYPT 2017

**9th International Conference on Cryptology in Africa, Dakar, Senegal, May 24–26, 2017**

Africacrypt is the annual International Conference on the Theory and Applications of Security and Cryptography.

## General Chairs

| | |
|---|---|
| Mamadou Sangharé | Université Cheikh Anta Diop de Dakar, Senegal |
| Djiby Sow | Université Cheikh Anta Diop de Dakar, Senegal |
| Abdoul Aziz Ciss | École Polytechnique de Thiès, Senegal |

## Program Chairs

| | |
|---|---|
| Marc Joye | NXP Semiconductors, USA |
| Abderrahmane Nitaj | Université de Caen, France |

## Program Committee

| | |
|---|---|
| Riham Altawy | University of Waterloo, Canada |
| Muhammad R.K. Ariffin | UPM Kuala Lumpur, Malaysia |
| Abdelhak Azhari | Université de Casablanca, Morocco |
| Hussain Benazza | Université de Meknes, Morocco |
| Colin Boyd | NTNU, Norway |
| Dario Catalano | Università di Catania, Italy |
| Pierre-Louis Cayrel | Université Saint Etienne, France |
| Sherman S.M. Chow | CU Hong Kong, SAR China |
| Nadia El Mrabet | EMSE, France |
| Pierre-Alain Fouque | Université Rennes I, France |
| Georg Fuchsbauer | ENS Paris, France |
| Jens Groth | University College London, UK |
| Javier Herranz | Universidad Politècnica de Catalunya, Spain |
| Tetsu Iwata | Nagoya University, Japan |
| Saqib Kakvi | University of Bristol, UK |
| Seny Kamara | Brown University, USA |
| Fabien Laguillaumie | Université de Lyon I, France |
| Mark Manulis | University of Surrey, UK |
| Tarik Moataz | Brown University, USA |
| Ayoub Otmani | Université de Rouen, France |

| | |
|---|---|
| Thomas Peters | UCL, Belgium |
| Tajje-eddine Rachidi | Al Akhawayn University in Ifrane, Morocco |
| Vanishree Rao | PARC, USA |
| Magdy Saeb | Arab Academy for Science, Egypt |
| Rei Safavi-Naini | University of Calgary, Canada |
| Kazue Sako | NEC, Japan |
| Palash Sarkar | Indian Statistical Institute, India |
| Peter Schwabe | Radboud Universiteit, The Netherlands |
| Francesco Sica | Nazarbayev University, Kazakhstan |
| Djiby Sow | Université de Dakar, Senegal |
| François-Xavier Standaert | UCL, Belgium |
| Willy Susilo | University of Wollongong, Australia |
| Christine Swart | University of Cape Town, South Africa |
| Joseph Tonien | University of Wollongong, Australia |
| Amr M. Youssef | Concordia University, Canada |

## External Reviewers

Ali Akhavi
Lejla Batina
Christof Beierle
Olivier Blazy
Andrea Cerulli
Qian Chen
Noureddine Chikouche
Abdoul Aziz Ciss
Michael Clear
Edouard Cuvelier
Gareth Davies
Julien Devigne
Dario Fiore
Ryo Furukawa
Romain Gay
Benoît Gérard
Essam Ghadafi
Aurore Guillevic
Mohammad Hajiabadi
Tsuchida Hikaru
Vincenzo Iovino
Sune K. Jakobsen
Jérémy Jean
Abdel Alim Kamal
Sabyasachi Karati
Ahmed Abdel Khalek
Elena Kirshanova
Stefan Koelbl
François Koeune
Baptiste Lambin
Liran Lerman
Fuchun Lin
Mary Maller
Paz Morillo
Thierry Mefenza Nountu
Kazuma Ohara
Michele Orrù
Romain Poussier
Raghvendra Rohit
Olivier Sanders
Ben Smith
Martin Strand
Isamu Teranishi
Nicolas Thériault
Yosuke Todo
Mohamed Tolba
Christine van Vredendaal
Vesselin Velichkov
Alexandre Wallet
Fredrich Wiemer
Yongjun Zhao

# Contents