Lecture Notes in Computer Science **14064**

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Nadia El Mrabet · Luca De Feo ·
Sylvain Duquesne
Editors

Progress in Cryptology - AFRICACRYPT 2023

14th International Conference
on Cryptology in Africa, Sousse, Tunisia, July 19–21, 2023
Proceedings

Springer

Editors
Nadia El Mrabet
EMSE
Saint-Étienne, France

Luca De Feo
IBM Research Europe
Rüschlikon, Switzerland

Sylvain Duquesne
Université de Rennes 1
Rennes Cedex, France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-37678-8 ISBN 978-3-031-37679-5 (eBook)
https://doi.org/10.1007/978-3-031-37679-5

Preface

This volume contains the papers accepted for presentation at Africacrypt 2023, the 14th International Conference on the Theory and Application of Cryptographic Techniques in Africa. The aim of this series of conferences is to provide an international forum for practitioners and researchers from industry, academia, and government agencies for a discussion of all forms of cryptography and its applications. The initiative of organizing Africacrypt started in 2008 and it was first held in Morocco. Subsequent yearly events were held in Tunisia, South Africa, Senegal, Morocco, Egypt and Tunisia. This year, Africacrypt 2023 is organized by the University of Monastir and the Tunisian Mathematical Society in cooperation with the International Association for Cryptologic Research (IACR). It was held in Sousse, during July 19–21, under the high patronage of the Tunisian minister of communication technologies.

We received 59 submissions authored by researchers from countries from all over the world. After a double-blind reviewing process that included online discussion and involved 47 Program Committee members and 23 external reviewers, we decided to accept 21 papers resulting in an acceptance rate of around 35%. All submitted papers received at least three reviews. We thank the Program Committee and the external reviewers for their diligent work and fruitful discussions and we thank the authors of all submitted papers for supporting the conference.

The conference program featured three keynote speakers, Ward Beullens from IBM Research Europe, Switzerland, Anne Canteaut from INRIA Paris, France and Koray Karabina from the National Research Council of Canada. We were happy that they agreed to attend and deliver their keynotes physically. The technical program was also enriched by a poster session organized by Abderrahmane Nitaj and Hoda Alkhzaimi. We thank them for taking this part of the program fully out of our hands and taking care of submissions, final versions, and chairing the poster session. A Capture the Flag (CTF) competition was introduced in the conference this year and was organized by Souheib Youssfi, Alyssa Berriche and Ahmed Belkahla.

The General Chairs, Leila Ben Abdelghani from the University of Monastir, Tunisia and Loubna Ghammam from ITK Engineering GmbH (Bosch), Germany, were a pleasure to work with. We thank the staff at Springer for their help with the proceedings production. Without our sponsors, in particular the Technology Innovation Institute from Abu Dhabi as a platinum sponsor, not all of the support for speakers and local organization facilities would have been possible and we thank them for that.

Acting as program chairs for Africacrypt 2023 was a privilege and a great experience, thanks go to all those people who helped us make this conference a big success.

May 2023

Luca De Feo
Sylvain Duquesne
Nadia El Mrabet

Organization

General Chairs

Leila Ben Abdelghani	University of Monastir, Tunisia
Loubna Ghammam	ITK Engineering GmbH (Bosch), Germany

Program Chairs

Nadia El Mrabet	École des Mines de Saint-Étienne, France
Luca De Feo	IBM Research Europe, Switzerland
Sylvain Duquesne	University of Rennes, France

Invited Speakers

Ward Beullens	IBM Research Europe, Switzerland
Anne Canteaut	INRIA Paris, France
Koray Karabina	National Research Council, Canada

Steering Committee

Souheib Yousfi (Chair)	University of Carthage, Tunisia
Nizar Kerkeni	University of Monastir, Tunisia
Lina Mortajine	ITK Engineering GmbH (Bosch), Germany
Abderrahmane Nitaj	University of Caen Normandie, France
Sami Omar	University of Bahrain, Bahrain
Amal Samti	University of Monastir, Tunisia

Program Committee

Riham AlTawy	University of Victoria, Canada
Laila El Aimani	University of Caddi Ayyad, Morocco
Hoda Alkhzaimi	NYU Abu Dhabi, United Arab Emirates

Greg Alpar	Open University, The Netherlands
Kevin Atighechi	University of Clermont-Ferrand, France
Hatem M. Bahig	Ain Shams University, Egypt
Hussain Benazza	UMI, ENSAM Meknes, Morocco
Shivam Bhasin	Temasek Lab, Nanyang Technological University, Singapore
Sebastien Canard	Orange Labs, France
Suvradip Chakraborty	ETH, Switzerland
Chitchanok Chuengsatiansup	University of Melbourne, Australia
Tingting Cui	HangZhou DianZi University, China
Joan Daemen	Radboud University, The Netherlands
Youssef El Housni	ConsenSys R&D, France
Georgios Fotiadis	University of Luxembourg
Emmanuel Fouotsa	University of Bamenda, Cameroon
Gina Gallegos-Garcia	Instituto Politécnico Nacional, Mexico
Romain Gay	IBM Research, Switzerland
Loubna Ghammam	ITK Engineering Gmbh (Bosch), Germany
Satrajit Ghosh	IIT Kharagpur, India
Lorenzo Grassi	Radboud University, The Netherlands
Javier Herranz	Universitat Politécnica de Catalunya, Spain
Akinori Hosoyamada	NTT, Japan
Sorina Ionica	University of Picardie, France
Juliane Kramer	TU Darmstadt, Germany
Fabien Laguillaumie	University of Montpellier, France
Patrick Longa	Microsoft Research, Redmond, US
Marc Manzano	SandboxAQ, Spain
Sarah McCarthy	University of Waterloo, Canada
Marine Minier	Université de Lorraine, France
Mainack Mondal	Indian Institute of Technology (IIT), India
Abderrahmane Nitaj	University of Caen Normandie, France
Sami Omar	University of Bahrain, Bahrain
Yanbin Pan	Chinese Academy of Science, China
Sikhar Patranabis	IBM Research, India
Christophe Petit	University of Birmingham, UK
Elizabeth A. Quaglia	Royal Holloway, University of London, UK
Divya Ravi	Aarhus University, Denmark
Joost Renes	NXP, The Netherlands
Yann Rotella	Université Paris-Saclay, France
Simona Samardjiska	Radboud University, The Netherlands
Ali Aydin Selcuk	TOBB University of Economics and Technology, Turkey
Dave Singelee	KU Leuven, Belgium

Djiby Sow	University of Dakar, Senegal
Pontelimon Stanica	Naval Postgraduate School, Monterey, USA
Vanessa Vitse	University of Grenoble, France
Souheib Yousfi	University of Carthage, Tunisia

Additional Reviewers

Khalid Abdelmoumen
Ismail Afia
Barbara Jiabao Benedikt
Harishma Boyapally
Guilhem Castagnos
Marwa Chaieb
Alfonso Francisco De Abiega L'Eglisse
Kevin Andrae Delgado Vargas
Siemen Dhooghe
Sayon Duttagupta
Samed Düzlü
Paul Frixons
Koustabh Ghosh
Tchoffo Saha Gustave
Çağdaş Gül
Jodie Knapp
Matthieu Lequesne
Soundes Marzougui
Lina Mortajine
Georgio Nicolas
Jean-Baptiste Orfila
Aurel Page
Santanu Sarkar
Ugur Sen
Ferdinand Sibleyras
Marloes Venema
Yanhong Xu
Trevor Yap
Steven Yue
Murat Burhan İlter

Contents

Cryptanalysis

Blockchain

Lattice-Based Cryptography

Implementations

Theory